Google Inc. et al v. Egger et al

Doc. 436 Att. 1

EXHIBIT I

Dockets.Justia.com

PROVIDED BY
FindLaw
WWW.FINDLAW.COM

U.S. Department of Justice

Washington, D.C. 20530

January 19, 2006

LEGAL AUTHORITIES SUPPORTING THE ACTIVITIES OF THE NATIONAL SECURITY AGENCY DESCRIBED BY THE PRESIDENT

As the President has explained, since shortly after the attacks of September 11, 2001, he has authorized the National Security Agency ("NSA") to intercept international communications into and out of the United States of persons linked to al Qaeda or related terrorist organizations. The purpose of these intercepts is to establish an early warning system to detect and prevent another catastrophic terrorist attack on the United States. This paper addresses, in an unclassified form, the legal basis for the NSA activities described by the President ("NSA activities").

SUMMARY

On September 11, 2001, the al Qaeda terrorist network launched the deadliest foreign attack on American soil in history. Al Qaeda's leadership repeatedly has pledged to attack the United States again at a time of its choosing, and these terrorist organizations continue to pose a grave threat to the United States. In response to the September 11th attacks and the continuing threat, the President, with broad congressional approval, has acted to protect the Nation from another terrorist attack. In the immediate aftermath of September 11th, the President promised that "[w]e will direct every resource at our command—every means of diplomacy, every tool of intelligence, every tool of law enforcement, every financial influence, and every weapon of war—to the destruction of and to the defeat of the global terrorist network." President Bush Address to a Joint Session of Congress (Sept. 20, 2001). The NSA activities are an indispensable aspect of this defense of the Nation. By targeting the international communications into and out of the United States of persons reasonably believed to be linked to al Qaeda, these activities provide the United States with an early warning system to help avert the next attack. For the following reasons, the NSA activities are lawful and consistent with civil liberties.

The NSA activities are supported by the President's well-recognized inherent constitutional authority as Commander in Chief and sole organ for the Nation in foreign affairs to conduct warrantless surveillance of enemy forces for intelligence purposes to detect and disrupt armed attacks on the United States. The President has the chief responsibility under the Constitution to protect America from attack, and the Constitution gives the President the authority necessary to fulfill that solemn responsibility. The President has made clear that he will exercise all authority available to him, consistent with the Constitution, to protect the people of the United States.

In the specific context of the current armed conflict with al Qaeda and related terrorist organizations, Congress by statute has confirmed and supplemented the President's recognized authority under Article II of the Constitution to conduct such warrantless surveillance to prevent further catastrophic attacks on the homeland. In its first legislative response to the terrorist attacks of September 11th, Congress authorized the President to "use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks" of September 11th in order to prevent "any future acts of international terrorism against the United States." Authorization for Use of Military Force, Pub. L. No. 107-40, § 2(a), 115 Stat. 224, 224 (Sept. 18, 2001) (reported as a note to 50 U.S.C.A. § 1541) ("AUMF"). History conclusively demonstrates that warrantless communications intelligence targeted at the enemy in time of armed conflict is a traditional and fundamental incident of the use of military force authorized by the AUMF. The Supreme Court's interpretation of the AUMF in *Hamdi v. Rumsfeld*, 542 U.S. 507 (2004), confirms that Congress in the AUMF gave its express approval to the military conflict against al Qaeda and its allies and thereby to the President's use of all traditional and accepted incidents of force in this current military conflict—including warrantless electronic surveillance to intercept enemy communications both at home and abroad. This understanding of the AUMF demonstrates Congress's support for the President's authority to protect the Nation and, at the same time, adheres to Justice O'Connor's admonition that "a state of war is not a blank check for the President," *Hamdi*, 542 U.S. at 536 (plurality opinion), particularly in view of the narrow scope of the NSA activities.

The AUMF places the President at the zenith of his powers in authorizing the NSA activities. Under the tripartite framework set forth by Justice Jackson in *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 635-38 (1952) (Jackson, J., concurring), Presidential authority is analyzed to determine whether the President is acting in accordance with congressional authorization (category I), whether he acts in the absence of a grant or denial of authority by Congress (category II), or whether he uses his own authority under the Constitution to take actions incompatible with congressional measures (category III). Because of the broad authorization provided in the AUMF, the President's action here falls within category I of Justice Jackson's framework. Accordingly, the President's power in authorizing the NSA activities is at its height because he acted "pursuant to an express or implied authorization of Congress," and his power "includes all that he possesses in his own right plus all that Congress can delegate." *Id.* at 635.

The NSA activities are consistent with the preexisting statutory framework generally applicable to the interception of communications in the United States—the Foreign Intelligence Surveillance Act ("FISA"), as amended, 50 U.S.C. §§ 1801-1862 (2000 & Supp. II 2002), and relevant related provisions in chapter 119 of title 18.[1] Although FISA generally requires judicial approval of electronic surveillance, FISA also contemplates that Congress may authorize such surveillance by a statute other than FISA. *See* 50 U.S.C. § 1809(a) (prohibiting any person from intentionally "engag[ing] . . . in electronic surveillance under color of law except as authorized

[1] Chapter 119 of title 18, which was enacted by Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended, 18 U.S.C. §§ 2510-2521 (2000 & West Supp. 2005), is often referred to as "Title III."

by statute"). The AUMF, as construed by the Supreme Court in *Hamdi* and as confirmed by the history and tradition of armed conflict, is just such a statute. Accordingly, electronic surveillance conducted by the President pursuant to the AUMF, including the NSA activities, is fully consistent with FISA and falls within category I of Justice Jackson's framework.

Even if there were ambiguity about whether FISA, read together with the AUMF, permits the President to authorize the NSA activities, the canon of constitutional avoidance requires reading these statutes in harmony to overcome any restrictions in FISA and Title III, at least as they might otherwise apply to the congressionally authorized armed conflict with al Qaeda. Indeed, were FISA and Title III interpreted to impede the President's ability to use the traditional tool of electronic surveillance to detect and prevent future attacks by a declared enemy that has already struck at the homeland and is engaged in ongoing operations against the United States, the constitutionality of FISA, as applied to that situation, would be called into very serious doubt. In fact, if this difficult constitutional question had to be addressed, FISA would be unconstitutional as applied to this narrow context. Importantly, the FISA Court of Review itself recognized just three years ago that the President retains constitutional authority to conduct foreign surveillance apart from the FISA framework, and the President is certainly entitled, at a minimum, to rely on that judicial interpretation of the Constitution and FISA.

Finally, the NSA activities fully comply with the requirements of the Fourth Amendment. The interception of communications described by the President falls within a well-established exception to the warrant requirement and satisfies the Fourth Amendment's fundamental requirement of reasonableness. The NSA activities are thus constitutionally permissible and fully protective of civil liberties.

BACKGROUND

A. THE ATTACKS OF SEPTEMBER 11, 2001

On September 11, 2001, the al Qaeda terrorist network launched a set of coordinated attacks along the East Coast of the United States. Four commercial jetliners, each carefully selected to be fully loaded with fuel for a transcontinental flight, were hijacked by al Qaeda operatives. Two of the jetliners were targeted at the Nation's financial center in New York and were deliberately flown into the Twin Towers of the World Trade Center. The third was targeted at the headquarters of the Nation's Armed Forces, the Pentagon. The fourth was apparently headed toward Washington, D.C., when passengers struggled with the hijackers and the plane crashed in Shanksville, Pennsylvania. The intended target of this fourth jetliner was evidently the White House or the Capitol, strongly suggesting that its intended mission was to strike a decapitation blow on the Government of the United States—to kill the President, the Vice President, or Members of Congress. The attacks of September 11th resulted in approximately 3,000 deaths—the highest single-day death toll from hostile foreign attacks in the Nation's history. These attacks shut down air travel in the United States, disrupted the Nation's financial markets and government operations, and caused billions of dollars in damage to the economy.

On September 14, 2001, the President declared a national emergency "by reason of the terrorist attacks at the World Trade Center, New York, New York, and the Pentagon, and the continuing and immediate threat of further attacks on the United States." Proclamation No. 7463, 66 Fed. Reg. 48,199 (Sept. 14, 2001). The same day, Congress passed a joint resolution authorizing the President "to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks" of September 11th, which the President signed on September 18th. AUMF § 2(a). Congress also expressly acknowledged that the attacks rendered it "necessary and appropriate" for the United States to exercise its right "to protect United States citizens both at home and abroad," and in particular recognized that "the President has authority under the Constitution to take action to deter and prevent acts of international terrorism against the United States." *Id.* pmbl. Congress emphasized that the attacks "continue to pose an unusual and extraordinary threat to the national security and foreign policy of the United States." *Id.* The United States also launched a large-scale military response, both at home and abroad. In the United States, combat air patrols were immediately established over major metropolitan areas and were maintained 24 hours a day until April 2002. The United States also immediately began plans for a military response directed at al Qaeda's base of operations in Afghanistan. Acting under his constitutional authority as Commander in Chief, and with the support of Congress, the President dispatched forces to Afghanistan and, with the assistance of the Northern Alliance, toppled the Taliban regime.

As the President made explicit in his Military Order of November 13, 2001, authorizing the use of military commissions to try terrorists, the attacks of September 11th "created a state of armed conflict." Military Order § 1(a), 66 Fed. Reg. 57,833 (Nov. 13, 2001). Indeed, shortly after the attacks, NATO—for the first time in its 46-year history—invoked article 5 of the North Atlantic Treaty, which provides that an "armed attack against one or more of [the parties] shall be considered an attack against them all." North Atlantic Treaty, Apr. 4, 1949, art. 5, 63 Stat. 2241, 2244, 34 U.N.T.S. 243, 246; *see also* Statement by NATO Secretary General Lord Robertson (Oct. 2, 2001), *available at* http://www.nato.int/docu/speech/2001/s011002a.htm ("[I]t has now been determined that the attack against the United States on 11 September was directed from abroad and shall therefore be regarded as an action covered by Article 5 of the Washington Treaty . . . ."). The President also determined in his Military Order that al Qaeda and related terrorists organizations "possess both the capability and the intention to undertake further terrorist attacks against the United States that, if not detected and prevented, will cause mass deaths, mass injuries, and massive destruction of property, and may place at risk the continuity of the operations of the United States Government," and concluded that "an extraordinary emergency exists for national defense purposes." Military Order, § 1(c), (g), 66 Fed. Reg. at 57,833-34.

B. THE NSA ACTIVITIES

Against this unfolding background of events in the fall of 2001, there was substantial concern that al Qaeda and its allies were preparing to carry out another attack within the United States. Al Qaeda had demonstrated its ability to introduce agents into the United States undetected and to perpetrate devastating attacks, and it was suspected that additional agents were likely already in position within the Nation's borders. As the President has explained, unlike a conventional enemy, al Qaeda has infiltrated "our cities and communities and communicated from here in America to plot and plan with bin Laden's lieutenants in Afghanistan, Pakistan and elsewhere." Press Conference of President Bush (Dec. 19, 2005), *available at* http://www.white-house.gov/news/releases/2005/12/20051219-2.html ("President's Press Conference"). To this day, finding al Qaeda sleeper agents in the United States remains one of the paramount concerns in the War on Terror. As the President has explained, "[t]he terrorists want to strike America again, and they hope to inflict even more damage than they did on September the 11th." *Id.*

The President has acknowledged that, to counter this threat, he has authorized the NSA to intercept international communications into and out of the United States of persons linked to al Qaeda or related terrorist organizations. The same day, the Attorney General elaborated and explained that in order to intercept a communication, there must be "a reasonable basis to conclude that one party to the communication is a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda." Press Briefing by Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence, *available at* http://www.whitehouse.gov/news/releases/2005/12/20051219-1.html (Dec. 19, 2005) (statement of Attorney General Gonzales). The purpose of these intercepts is to establish an early warning system to detect and prevent another catastrophic terrorist attack on the United States. The President has stated that the NSA activities "ha[ve] been effective in disrupting the enemy, while safeguarding our civil liberties." President's Press Conference.

The President has explained that the NSA activities are "critical" to the national security of the United States. *Id.* Confronting al Qaeda "is not simply a matter of [domestic] law enforcement"—we must defend the country against an enemy that declared war against the United States. *Id.* To "effectively detect enemies hiding in our midst and prevent them from striking us again . . . we must be able to act fast and to detect conversations [made by individuals linked to al Qaeda] so we can prevent new attacks." *Id.* The President pointed out that "a two-minute phone conversation between somebody linked to al Qaeda here and an operative overseas could lead directly to the loss of thousands of lives." *Id.* The NSA activities are intended to help "connect the dots" between potential terrorists. *Id.* In addition, the Nation is facing "a different era, a different war . . . people are changing phone numbers . . . and they're moving quick[ly]." *Id.* As the President explained, the NSA activities "enable[] us to move faster and quicker. And that's important. We've got to be fast on our feet, quick to detect and prevent." *Id.* "This is an enemy that is quick and it's lethal. And sometimes we have to move very, very quickly." *Id.* FISA, by contrast, is better suited "for long-term monitoring." *Id.*

As the President has explained, the NSA activities are "carefully reviewed approximately every 45 days to ensure that [they are] being used properly." *Id.* These activities are reviewed for legality by the Department of Justice and are monitored by the General Counsel and Inspector General of the NSA to ensure that civil liberties are being protected. *Id.* Leaders in Congress from both parties have been briefed more than a dozen times on the NSA activities.

C. The Continuing Threat Posed by al Qaeda

Before the September 11th attacks, al Qaeda had promised to attack the United States. In 1998, Osama bin Laden declared a "religious" war against the United States and urged that it was the moral obligation of all Muslims to kill U.S. civilians and military personnel. *See* Statement of Osama bin Laden, Ayman al-Zawahiri, et al., *Fatwah Urging Jihad Against Americans*, published in Al-Quds al-'Arabi (Feb. 23, 1998) ("To kill the Americans and their allies—civilians and military—is an individual duty for every Muslim who can do it in any country in which it is possible to do it, in order to liberate the al-Aqsa Mosque and the holy mosque from their grip, and in order for their armies to move out of all the lands of Islam, defeated and unable to threaten any Muslim."). Al Qaeda carried out those threats with a vengeance; they attacked the U.S.S. Cole in Yemen, the United States Embassy in Nairobi, and finally the United States itself in the September 11th attacks.

It is clear that al Qaeda is not content with the damage it wrought on September 11th. As recently as December 7, 2005, Ayman al-Zawahiri professed that al Qaeda "is spreading, growing, and becoming stronger," and that al Qaeda is "waging a great historic battle in Iraq, Afghanistan, Palestine, and even in the Crusaders' own homes." Ayman al-Zawahiri, videotape released on Al-Jazeera television network (Dec. 7, 2005). Indeed, since September 11th, al Qaeda leaders have repeatedly promised to deliver another, even more devastating attack on America. *See, e.g.*, Osama bin Laden, videotape released on Al-Jazeera television network (Oct. 24, 2004) (warning United States citizens of further attacks and asserting that "your security is in your own hands"); Osama bin Laden, videotape released on Al-Jazeera television network (Oct. 18, 2003) ("We, God willing, will continue to fight you and will continue martyrdom operations inside and outside the United States . . . ."); Ayman Al-Zawahiri, videotape released on the Al-Jazeera television network (Oct. 9, 2002) ("I promise you [addressing the 'citizens of the United States'] that the Islamic youth are preparing for you what will fill your hearts with horror"). Given that al Qaeda's leaders have repeatedly made good on their threats and that al Qaeda has demonstrated its ability to insert foreign agents into the United States to execute attacks, it is clear that the threat continues. Indeed, since September 11th, al Qaeda has staged several large-scale attacks around the world, including in Indonesia, Madrid, and London, killing hundreds of innocent people.

Analysis

I. The President Has Inherent Constitutional Authority To Order Warrantless Foreign Intelligence Surveillance

As Congress expressly recognized in the AUMF, "the President has authority under the Constitution to take action to deter and prevent acts of international terrorism against the United States," AUMF pmbl., especially in the context of the current conflict. Article II of the Constitution vests in the President all executive power of the United States, including the power to act as Commander in Chief of the Armed Forces, *see* U.S. Const. art. II, § 2, and authority over the conduct of the Nation's foreign affairs. As the Supreme Court has explained, "[t]he President is the sole organ of the nation in its external relations, and its sole representative with foreign nations." *United States v. Curtiss-Wright Export Corp.*, 299 U.S. 304, 319 (1936) (internal quotation marks and citations omitted). In this way, the Constitution grants the President inherent power to protect the Nation from foreign attack, *see, e.g.*, *The Prize Cases,* 67 U.S. (2 Black) 635, 668 (1863), and to protect national security information, *see, e.g.*, *Department of the Navy v. Egan,* 484 U.S. 518, 527 (1988).

To carry out these responsibilities, the President must have authority to gather information necessary for the execution of his office. The Founders, after all, intended the federal Government to be clothed with all authority necessary to protect the Nation. *See, e.g.*, *The Federalist* No. 23, at 147 (Alexander Hamilton) (Jacob E. Cooke ed. 1961) (explaining that the federal Government will be "cloathed with all the powers requisite to the complete execution of its trust"); *id.* No. 41, at 269 (James Madison) ("Security against foreign danger is one of the primitive objects of civil society . . . . The powers requisite for attaining it must be effectually confided to the federal councils."). Because of the structural advantages of the Executive Branch, the Founders also intended that the President would have the primary responsibility and necessary authority as Commander in Chief and Chief Executive to protect the Nation and to conduct the Nation's foreign affairs. *See, e.g.*, *The Federalist* No. 70, at 471-72 (Alexander Hamilton); *see also Johnson v. Eisentrager,* 339 U.S. 763, 788 (1950) ("this [constitutional] grant of war power includes all that is necessary and proper for carrying these powers into execution") (citation omitted). Thus, it has been long recognized that the President has the authority to use secretive means to collect intelligence necessary for the conduct of foreign affairs and military campaigns. *See, e.g.*, *Chicago & S. Air Lines v. Waterman S.S. Corp.*, 333 U.S. 103, 111 (1948) ("The President, both as Commander-in-Chief and as the Nation's organ for foreign affairs, has available intelligence services whose reports are not and ought not to be published to the world."); *Curtiss-Wright,* 299 U.S. at 320 ("He has his confidential sources of information. He has his agents in the form of diplomatic, consular and other officials."); *Totten v. United States,* 92 U.S. 105, 106 (1876) (President "was undoubtedly authorized during the war, as commander-in-chief . . . to employ secret agents to enter the rebel lines and obtain information respecting the strength, resources, and movements of the enemy").

In reliance on these principles, a consistent understanding has developed that the President has inherent constitutional authority to conduct warrantless searches and surveillance within the United States for foreign intelligence purposes. Wiretaps for such purposes thus have been authorized by Presidents at least since the administration of Franklin Roosevelt in 1940. *See, e.g., United States v. United States District Court,* 444 F.2d 651, 669-71 (6th Cir. 1971) (reproducing as an appendix memoranda from Presidents Roosevelt, Truman, and Johnson). In a Memorandum to Attorney General Jackson, President Roosevelt wrote on May 21, 1940:

> You are, therefore, authorized and directed in such cases as you may approve, after investigation of the need in each case, to authorize the necessary investigation agents that they are at liberty to secure information by listening devices directed to the conversation or other communications of persons suspected of subversive activities against the Government of the United States, including suspected spies. You are requested furthermore to limit these investigations so conducted to a minimum and limit them insofar as

possible to aliens.

Id. at 670 (appendix A). President Truman approved a memorandum drafted by Attorney General Tom Clark in which the Attorney General advised that "it is as necessary as it was in 1940 to take the investigative measures" authorized by President Roosevelt to conduct electronic surveillance "in cases vitally affecting the domestic security." *Id.* Indeed, while FISA was being debated during the Carter Administration, Attorney General Griffin Bell testified that "the current bill recognizes no inherent power of the President to conduct electronic surveillance, and I want to interpolate here to say that *this does not take away the power [of] the President under the Constitution.*" Foreign Intelligence Electronic Surveillance Act of 1978: Hearings on H.R. 5764, H.R. 9745, H.R. 7308, and H.R. 5632 Before the Subcomm. on Legislation of the House Comm. on Intelligence, 95th Cong., 2d Sess. 15 (1978) (emphasis added); *see also Katz v. United States*, 389 U.S. 347, 363 (1967) (White, J., concurring) ("Wiretapping to protect the security of the Nation has been authorized by successive Presidents."); *cf.* Amending the Foreign Intelligence Surveillance Act: Hearings Before the House Permanent Select Comm. on Intelligence,103d Cong. 2d Sess. 61 (1994) (statement of Deputy Attorney General Jamie S. Gorelick) ("[T]he Department of Justice believes, and the case law supports, that the President has inherent authority to conduct warrantless physical searches for foreign intelligence purposes . . . .").

The courts uniformly have approved this longstanding Executive Branch practice. Indeed, every federal appellate court to rule on the question has concluded that, even in peacetime, the President has inherent constitutional authority, consistent with the Fourth Amendment, to conduct searches for foreign intelligence purposes without securing a judicial warrant. *See In re Sealed Case,* 310 F.3d 717, 742 (Foreign Intel. Surv. Ct. of Rev. 2002) ("[A]ll the other courts to have decided the issue [have] held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information . . . . *We take for granted that the President does have that authority and, assuming that is so, FISA could not encroach on the President's constitutional power.*") (emphasis added); *accord, e.g., United States v. Truong Dinh Hung,* 629 F.2d 908 (4th Cir. 1980); *United States v. Butenko,* 494 F.2d 593 (3d Cir. 1974) (en banc); *United States v. Brown,* 484 F.2d 418 (5th Cir. 1973). *But cf. Zweibon v. Mitchell,* 516 F.2d 594 (D.C. Cir. 1975) (en banc) (dictum in plurality opinion suggesting that a warrant would be required even in a foreign intelligence investigation).

In *United States v. United States District Court,* 407 U.S. 297 (1972) (the "*Keith*" case), the Supreme Court concluded that the Fourth Amendment's warrant requirement applies to investigations of wholly *domestic* threats to security—such as domestic political violence and other crimes. But the Court in the *Keith* case made clear that it was not addressing the President's authority to conduct *foreign* intelligence surveillance without a warrant and that it was expressly reserving that question: "[T]he instant case requires no judgment on the scope of the President's surveillance power with respect to the activities of foreign powers, within or without this country." *Id.* at 308; *see also id.* at 321-22 & n.20 ("We have not addressed, and express no opinion as to, the issues which may be involved with respect to activities of foreign powers or their agents."). That *Keith* does not apply in the context of protecting against a foreign attack has been confirmed by the lower courts. After *Keith*, each of the three courts of appeals that have squarely considered the question have concluded—expressly taking the Supreme Court's decision into account—that the President has inherent authority to conduct warrantless surveillance in the foreign intelligence context. *See, e.g.*, *Truong Dinh Hung*, 629 F.2d at 913-14; *Butenko*, 494 F.2d at 603; *Brown*, 484 F.2d 425-26.

From a constitutional standpoint, foreign intelligence surveillance such as the NSA activities differs fundamentally from the domestic security surveillance at issue in *Keith*. As the Fourth Circuit observed, the President has uniquely strong constitutional powers in matters pertaining to foreign affairs and national security. "Perhaps most crucially, the executive branch not only has superior expertise in the area of foreign intelligence, it is also constitutionally designated as the pre-eminent authority in foreign affairs." *Truong*, 629 F.2d at 914; *see id.* at 913 (noting that "the needs of the executive are so compelling in the area of foreign intelligence, unlike the area of domestic security, that a uniform warrant requirement would . . . unduly frustrate the President in carrying out his foreign affairs responsibilities"); *cf. Haig v. Agee*, 453 U.S. 280, 292 (1981) ("Matters intimately related to foreign policy and national security are rarely proper subjects for judicial intervention.").[2]

The present circumstances that support recognition of the President's inherent constitutional authority to conduct the NSA activities are considerably stronger than were the circumstances at issue in the earlier courts of appeals cases that recognized this power. All of the cases described above addressed inherent executive authority under the foreign affairs power to conduct surveillance in a peacetime context. The courts in these cases therefore had no occasion even to consider the fundamental authority of the President, as Commander in Chief, to gather intelligence in the context of an ongoing armed conflict in which the United States already had suffered massive civilian casualties and in which the intelligence gathering efforts at issue were specifically designed to thwart further armed attacks. Indeed, intelligence gathering is particularly important in the current conflict, in which the enemy attacks largely through clandestine activities and which, as Congress recognized, "pose[s] an unusual and extraordinary threat," AUMF pmbl.

Among the President's most basic constitutional duties is the duty to protect the Nation from armed attack. The Constitution gives him all necessary authority to fulfill that responsibility. The courts thus have long acknowledged the President's inherent authority to take action to protect Americans abroad, *see, e.g.*, *Durand v. Hollins*, 8 F. Cas. 111, 112 (C.C.S.D.N.Y. 1860) (No. 4186), and to protect the Nation from attack, *see, e.g.*, *The Prize Cases*, 67 U.S. at 668. *See generally Ex parte Quirin*, 317 U.S. 1, 28 (1942) (recognizing that

[2] *Keith* made clear that one of the significant concerns driving the Court's conclusion in the domestic security context was the inevitable connection between perceived threats to domestic security and political dissent. As the Court explained: "Fourth Amendment protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs. The danger to political dissent is acute where the Government attempts to act under so vague a concept as the power to protect 'domestic security.'" *Keith*, 407 U.S. at 314; *see also id.* at 320 ("Security surveillances are especially sensitive because of the inherent vagueness of the domestic security concept, the necessarily broad and continuing nature of intelligence gathering, and the temptation to utilize such surveillances to oversee political dissent."). Surveillance of domestic groups raises a First Amendment concern that generally is not present when the subjects of the surveillance are foreign powers or their agents.

the President has authority under the Constitution "to direct the performance of those functions which may constitutionally be performed by the military arm of the nation in time of war," including "important incident[s] to the conduct of war," such as "the adoption of measures by the military command . . . to repel and defeat the enemy"). As the Supreme Court emphasized in the *Prize Cases*, if the Nation is invaded, the President is "bound to resist force by force"; "[h]e must determine what degree of force the crisis demands" and need not await congressional sanction to do so. *The Prize Cases,* 67 U.S. at 670; *see also Campbell v. Clinton,* 203 F.3d 19, 27 (D.C. Cir. 2000) (Silberman, J., concurring) ("[T]he *Prize Cases* . . . stand for the proposition that the President has independent authority to repel aggressive acts by third parties even without specific congressional authorization, and courts may not review the level of force selected."); *id.* at 40 (Tatel, J., concurring) ("[T]he President, as commander in chief, possesses emergency authority to use military force to defend the nation from attack without obtaining prior congressional approval."). Indeed, "in virtue of his rank as head of the forces, [the President] has certain powers and duties with which Congress cannot interfere." *Training of British Flying Students in the United States,* 40 Op. Att'y Gen. 58, 61 (1941) (Attorney General Robert H. Jackson) (internal quotation marks omitted). In exercising his constitutional powers, the President has wide discretion, consistent with the Constitution, over the methods of gathering intelligence about the Nation's enemies in a time of armed conflict.

II. THE AUMF CONFIRMS AND SUPPLEMENTS THE PRESIDENT'S INHERENT POWER TO USE WARRANTLESS SURVEILLANCE AGAINST THE ENEMY IN THE CURRENT ARMED CONFLICT

In the Authorization for Use of Military Force enacted in the wake of September 11th, Congress confirms and supplements the President's constitutional authority to protect the Nation, including through electronic surveillance, in the context of the current post-September 11th armed conflict with al Qaeda and its allies. The broad language of the AUMF affords the President, at a minimum, discretion to employ the traditional incidents of the use of military force. The history of the President's use of warrantless surveillance during armed conflicts demonstrates that the NSA surveillance described by the President is a fundamental incident of the use of military force that is necessarily included in the AUMF.

A. THE TEXT AND PURPOSE OF THE AUMF AUTHORIZE THE NSA ACTIVITIES

On September 14, 2001, in its first legislative response to the attacks of September 11th, Congress gave its express approval to the President's military campaign against al Qaeda and, in the process, confirmed the well-accepted understanding of the President's Article II powers. *See* AUMF § 2(a).[3] In the preamble to the AUMF, Congress stated that "the President has authority under the Constitution to take action to deter and prevent acts of international terrorism against the United States," AUMF pmbl., and thereby acknowledged the President's inherent constitutional authority to defend the United States. This clause "constitutes an extraordinarily

[3] America's military response began before the attacks of September 11th had been completed. *See The 9/11 Commission Report* 20 (2004). Combat air patrols were established and authorized "to engage inbound aircraft if they could verify that the aircraft was hijacked." *Id.* at 42.

sweeping recognition of independent presidential *constitutional* power to employ the war power to combat terrorism." Michael Stokes Paulsen, Youngstown *Goes to War,* 19 Const. Comment. 215, 252 (2002). This striking recognition of presidential authority cannot be discounted as the product of excitement in the immediate aftermath of September 11th, for the same terms were repeated by Congress more than a year later in the Authorization for Use of Military Force Against Iraq Resolution of 2002. Pub. L. No. 107-243, pmbl., 116 Stat. 1498, 1500 (Oct. 16, 2002) ("[T]he President has authority under the Constitution to take action in order to deter and prevent acts of international terrorism against the United States . . . ."). In the context of the conflict with al Qaeda and related terrorist organizations, therefore, Congress has acknowledged a broad executive authority to "deter and prevent" further attacks against the United States.

The AUMF passed by Congress on September 14, 2001, does not lend itself to a narrow reading. Its expansive language authorizes the President "to use *all necessary and appropriate force* against those nations, organizations, or persons *he determines* planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001." AUMF § 2(a) (emphases added). In the field of foreign affairs, and particularly that of war powers and national security, congressional enactments are to be broadly construed where they indicate support for authority long asserted and exercised by the Executive Branch. *See, e.g., Haig v. Agee*, 453 U.S. 280, 293-303 (1981); *United States ex rel. Knauff v. Shaughnessy*, 338 U.S. 537, 543-45 (1950); *cf. Loving v. United States,* 517 U.S. 748, 772 (1996) (noting that the usual "limitations on delegation [of congressional powers] do not apply" to authorizations linked to the Commander in Chief power); *Dames & Moore v. Regan*, 453 U.S. 654, 678-82 (1981) (even where there is no express statutory authorization for executive action, legislation in related field may be construed to indicate congressional acquiescence in that action). Although Congress's war powers under Article I, Section 8 of the Constitution empower Congress to legislate regarding the raising, regulation, and material support of the Armed Forces and related matters, rather than the prosecution of military campaigns, the AUMF indicates Congress's endorsement of the President's use of his constitutional war powers. This authorization transforms the struggle against al Qaeda and related terrorist organizations from what Justice Jackson called "a zone of twilight," in which the President and the Congress may have concurrent powers whose "distribution is uncertain," *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 637 (1952) (Jackson, J., concurring), into a situation in which the President's authority is at is maximum because "it includes all that he possesses in his own right plus all that Congress can delegate," *id.* at 635. With regard to these fundamental tools of warfare—and, as demonstrated below, warrantless electronic surveillance against the declared enemy is one such tool—the AUMF places the President's authority at its zenith under *Youngstown.*

It is also clear that the AUMF confirms and supports the President's use of those traditional incidents of military force against the enemy, wherever they may be—on United States soil or abroad. The nature of the September 11th attacks—launched on United States soil by foreign agents secreted in the United States—necessitates such authority, and the text of the AUMF confirms it. The operative terms of the AUMF state that the President is authorized to use force "in order to prevent any future acts of international terrorism against the United States," *id.*, an objective which, given the recent attacks within the Nation's borders and the continuing use of air defense throughout the country at the time Congress acted, undoubtedly contemplated the possibility of military action within the United States. The preamble, moreover, recites that the United States should exercise its rights "to protect United States citizens both *at home* and abroad." *Id.* pmbl. (emphasis added). To take action against those linked to the September 11th attacks involves taking action against individuals within the United States. The United States had been attacked on its own soil—not by aircraft launched from carriers several hundred miles away, but by enemy agents who had resided in the United States for months. A crucial responsibility of the President—charged by the AUMF and the Constitution—was and is to identify and attack those enemies, especially if they were in the United States, ready to strike against the Nation.

The text of the AUMF demonstrates in an additional way that Congress authorized the President to conduct warrantless electronic surveillance against the enemy. The terms of the AUMF not only authorized the President to "use all necessary and appropriate force" against those responsible for the September 11th attacks; it also authorized the President to "determine[]" the persons or groups responsible for those attacks and to take all actions necessary to prevent further attacks. AUMF § 2(a) ("the President is authorized to use all necessary and appropriate force against those nations, organizations, or persons *he determines* planned, authorized, committed, or aided the terrorist attacks that occurred on September 11th, 2001, or harbored such organizations or persons") (emphasis added). Of vital importance to the use of force against the enemy is locating the enemy and identifying its plans of attack. And of vital importance to identifying the enemy and detecting possible future plots was the authority to intercept communications to or from the United States of persons with links to al Qaeda or related terrorist organizations. Given that the agents who carried out the initial attacks resided in the United States and had successfully blended into American society and disguised their identities and intentions until they were ready to strike, the necessity of using the most effective intelligence gathering tools against such an enemy, including electronic surveillance, was patent. Indeed, Congress recognized that the enemy in this conflict poses an "unusual and extraordinary threat." AUMF pmbl.

The Supreme Court's interpretation of the scope of the AUMF in *Hamdi v. Rumsfeld*, 542 U.S. 507 (2004), strongly supports this reading of the AUMF. In *Hamdi*, five members of the Court found that the AUMF authorized the detention of an American within the United States, notwithstanding a statute that prohibits the detention of U.S. citizens "except pursuant to an Act of Congress," 18 U.S.C. § 4001(a). *See Hamdi*, 542 U.S. at 519 (plurality opinion); *id.* at 587 (Thomas, J., dissenting). Drawing on historical materials and "longstanding law-of-war principles," *id.* at 518-21, a plurality of the Court concluded that detention of combatants who fought against the United States as part of an organization "known to have supported" al Qaeda "is so fundamental and accepted an incident to war as to be an exercise of the 'necessary and appropriate force' Congress has authorized the President to use." *Id.* at 518; *see also id.* at 587 (Thomas, J., dissenting) (agreeing with the plurality that the joint resolution authorized the President to "detain those arrayed against our troops"); *accord Quirin*, 317 U.S. at 26-29, 38 (recognizing the President's authority to capture and try agents of the enemy in the United States even if they had never "entered the theatre or zone of active military operations"). Thus, even though the AUMF does not say anything expressly about detention, the Court nevertheless found that it satisfied section 4001(a)'s requirement that detention be congressionally authorized.

The conclusion of five Justices in *Hamdi* that the AUMF incorporates fundamental "incidents" of the use of military force makes clear that the absence of any specific reference to signals intelligence activities in the resolution is immaterial. *See Hamdi,* 542 U.S. at 519 ("[I]t is of no moment that the AUMF does not use specific language of detention.") (plurality opinion). Indeed, given the circumstances in which the AUMF was adopted, it is hardly surprising that Congress chose to speak about the President's authority in general terms. The purpose of the AUMF was for Congress to sanction and support the military response to the devastating terrorist attacks that had occurred just three days earlier. Congress evidently thought it neither necessary nor appropriate to attempt to catalog every specific aspect of the use of the forces it was authorizing and every potential preexisting statutory limitation on the Executive Branch. Rather than engage in that difficult and impractical exercise, Congress authorized the President, in general but intentionally broad terms, to use the traditional and fundamental incidents of war and to determine how best to identify and engage the enemy in the current armed conflict. Congress's judgment to proceed in this manner was unassailable, for, as the Supreme Court has recognized, even in normal times involving no major national security crisis, "Congress cannot anticipate and legislate with regard to every possible action the President may find it necessary to take." *Dames & Moore*, 453 U.S. at 678. Indeed, Congress often has enacted authorizations to use military force using general authorizing language that does not purport to catalogue in detail the specific powers the President may employ. The need for Congress to speak broadly in recognizing and augmenting the President's core constitutional powers over foreign affairs and military campaigns is of course significantly heightened in times of national emergency. *See Zemel v. Rusk,* 381 U.S. 1, 17 (1965) ("[B]ecause of the changeable and explosive nature of contemporary international relations . . . Congress—in giving the Executive authority over matters of foreign affairs—must of necessity paint with a brush broader than that it customarily wields in domestic areas.").

Hamdi thus establishes the proposition that the AUMF "clearly and unmistakably" authorizes the President to take actions against al Qaeda and related organizations that amount to "fundamental incident[s] of waging war." *Hamdi*, 542 U.S. at 519 (plurality opinion); *see also id.* at 587 (Thomas, J., dissenting). In other words, "*[t]he clear inference is that the AUMF authorizes what the laws of war permit.*" Curtis A. Bradley & Jack L. Goldsmith, *Congressional Authorization and the War on Terrorism*, 118 Harv. L. Rev. 2048, 2092 (2005) (emphasis added). Congress is presumed to be aware of the Supreme Court's precedents. Indeed, Congress recently enacted legislation in response to the Court's decision in *Rasul v. Bush*, 542 U.S. 466 (2004)—which was issued the same day as the *Hamdi* decision—removing habeas corpus jurisdiction over claims filed on behalf of confined enemy combatants held at Guantanamo Bay. Congress, however, has not expressed any disapproval of the Supreme Court's commonsense and plain-meaning interpretation of the AUMF in *Hamdi.*[4]

---

[4] This understanding of the AUMF is consistent with Justice O'Connor's admonition that "a state of war is not a blank check for the President," *Hamdi*, 542 U.S. at 536 (plurality opinion). In addition to constituting a fundamental and accepted incident of the use of military force, the NSA activities are consistent with the law of armed conflict principle that the use of force be necessary and proportional. *See* Dieter Fleck, *The Handbook of Humanitarian Law in Armed Conflicts* 115 (1995). The NSA activities are proportional because they are minimally invasive and narrow in scope, targeting only the international communications of persons reasonably believed to be linked to al Qaeda, and are designed to protect the Nation from a devastating attack.

B. WARRANTLESS ELECTRONIC SURVEILLANCE AIMED AT INTERCEPTING ENEMY COMMUNICATIONS HAS LONG BEEN RECOGNIZED AS A FUNDAMENTAL INCIDENT OF THE USE OF MILITARY FORCE

The history of warfare—including the consistent practice of Presidents since the earliest days of the Republic—demonstrates that warrantless intelligence surveillance against the enemy is a fundamental incident of the use of military force, and this history confirms the statutory authority provided by the AUMF. Electronic surveillance is a fundamental tool of war that must be included in any natural reading of the AUMF's authorization to use "all necessary and appropriate force."

As one author has explained:

> It is *essential* in warfare for a belligerent to be as fully informed as possible about the enemy—his strength, his weaknesses, measures taken by him and measures contemplated by him. This applies not only to military matters, but . . . anything which bears on and is material to his ability to wage the war in which he is engaged. *The laws of war recognize and sanction this aspect of warfare.*

Morris Greenspan, *The Modern Law of Land Warfare* 325 (1959) (emphases added); *see also* Memorandum for Members of the House Permanent Select Comm. on Intel., from Jeffrey H. Smith, *Re: Legal Authorities Regarding Warrantless Surveillance of U.S. Persons* 6 (Jan. 3, 2006) ("Certainly, the collection of intelligence is understood to be necessary to the execution of the war."). Similarly, article 24 of the Hague Regulations of 1907 expressly states that "the employment of measures necessary for obtaining information about the enemy and the country [is] considered permissible." *See also* L. Oppenheim, *International Law* vol. II § 159 (7th ed. 1952) ("War cannot be waged without all kinds of information, about the forces and the intentions of the enemy . . . . To obtain the necessary information, it has always been considered lawful to employ spies . . . ."); Joseph R. Baker & Henry G. Crocker, *The Laws of Land Warfare* 197 (1919) ("Every belligerent has a right . . . to discover the signals of the enemy and . . . to seek to procure information regarding the enemy through the aid of secret agents."); *cf.* J.M. Spaight, *War Rights on Land* 205 (1911) ("[E]very nation employs spies; were a nation so quixotic as to refrain from doing so, it might as well sheathe its sword for ever. . . . Spies . . . are indispensably necessary to a general; and, other things being equal, that commander will be victorious who has the best secret service.") (internal quotation marks omitted).

In accordance with these well-established principles, the Supreme Court has consistently recognized the President's authority to conduct intelligence activities. *See, e.g., Totten v. United States,* 92 U.S. 105, 106 (1876) (recognizing President's authority to hire spies); *Tenet v. Doe*, 544 U.S. 1 (2005) (reaffirming *Totten* and counseling against judicial interference with such matters); *see also Chicago & S. Air Lines v. Waterman S.S. Corp.*, 333 U.S. 103, 111 (1948) ("The President, both as Commander-in-Chief and as the Nation's organ for foreign affairs, has available intelligence services whose reports neither are not and ought not to be published to the world."); *United States v. Curtiss-Wright Export Corp.*, 299 U.S. 304, 320 (1936) (The President "has his confidential sources of information. He has his agents in the form of diplomatic, consular, and other officials."). Chief Justice John Marshall even described the gathering of intelligence as a military duty. *See Tatum v. Laird,* 444 F.2d 947, 952-53 (D.C. Cir. 1971) ("As Chief Justice John Marshall said of Washington, 'A general must be governed by his intelligence and must regulate his measures by his information. It is his duty to obtain correct information . . . . '") (quoting Foreword, U.S. Army Basic Field Manual, Vol. X, circa 1938), *rev'd on other grounds*, 408 U.S. 1 (1972).

The United States, furthermore, has a long history of wartime surveillance—a history that can be traced to George Washington, who "was a master of military espionage" and "made frequent and effective use of secret intelligence in the second half of the eighteenth century." Rhodri Jeffreys-Jones, *Cloak and Dollar: A History of American Secret Intelligence* 11 (2002); *see generally id.* at 11-23 (recounting Washington's use of intelligence); *see also Haig v. Agee*, 471 U.S. 159, 172 n.16 (1981) (quoting General Washington's letter to an agent embarking upon an intelligence mission in 1777: "The necessity of procuring good intelligence, is apparent and need not be further urged."). As President in 1790, Washington obtained from Congress a "secret fund" to deal with foreign dangers and to be spent at his discretion. Jeffreys-Jones, *supra*, at 22. The fund, which remained in use until the creation of the Central Intelligence Agency in the mid-twentieth century and gained "longstanding acceptance within our constitutional structure," *Halperin v. CIA,* 629 F.2d 144, 158-59 (D.C. Cir. 1980), was used "for all purposes to which a secret service fund should or could be applied for the public benefit," including "for persons sent publicly and secretly to search for important information, political or commercial," *id.* at 159 (quoting Statement of Senator John Forsyth, Cong. Debates 295 (Feb. 25, 1831)). *See also Totten,* 92 U.S. at 107 (refusing to examine payments from this fund lest the publicity make a "secret service" "impossible").

The interception of communications, in particular, has long been accepted as a fundamental method for conducting wartime surveillance. *See, e.g.*, Greenspan, *supra*, at 326 (accepted and customary means for gathering intelligence "include air reconnaissance and photography; ground reconnaissance; observation of enemy positions; *interception of enemy messages, wireless and other*; examination of captured documents; . . . and interrogation of prisoners and civilian inhabitants") (emphasis added). Indeed, since its independence, the United States has intercepted communications for wartime intelligence purposes and, if necessary, has done so within its own borders. During the Revolutionary War, for example, George Washington received and used to his advantage reports from American intelligence agents on British military strength, British strategic intentions, and British estimates of American strength. *See* Jeffreys-Jones, *supra*, at 13. One source of Washington's intelligence was intercepted British mail. *See* Central Intelligence Agency, *Intelligence in the War of Independence* 31, 32 (1997). In fact, Washington himself proposed that one of his Generals "contrive a means of opening [British letters] without breaking the seals, take copies of the contents, and then let them go on." *Id.* at 32 ("From that point on, Washington was privy to British intelligence pouches between New York and Canada."); *see generally* Final Report of the Select Committee to Study Governmental Operations with respect to Intelligence Activities (the "Church Committee"), S. Rep. No. 94-755, at Book VI, 9-17 (Apr. 23, 1976) (describing Washington's intelligence activities).

More specifically, warrantless electronic surveillance of wartime communications has been conducted in the United States since electronic communications have existed, *i.e.,* since at least the Civil War, when "[t]elegraph wiretapping was common, and an important intelligence source for both sides." G.J.A. O'Toole, *The Encyclopedia of American Intelligence and Espionage* 498 (1988). Confederate General J.E.B. Stuart even "had his own personal wiretapper travel along with him in the field" to intercept military telegraphic communications. Samuel Dash, et al., *The Eavesdroppers* 23 (1971); *see also* O'Toole, *supra*, at 121, 385-88, 496-98 (discussing Civil War surveillance methods such as wiretaps, reconnaissance balloons, semaphore interception, and cryptanalysis). Similarly, there was extensive use of electronic surveillance during the Spanish-American War. *See* Bruce W. Bidwell, *History of the Military Intelligence Division, Department of the Army General Staff*: 1775-1941, at 62 (1986). When an American expeditionary force crossed into northern Mexico to confront the forces of Pancho Villa in 1916, the Army "frequently intercepted messages of the regime in Mexico City or the forces contesting its rule." David Alvarez, *Secret Messages* 6-7 (2000). Shortly after Congress declared war on Germany in World War I, President Wilson (citing only his constitutional powers and the joint resolution declaring war) ordered the censorship of messages sent outside the United States via submarine cables, telegraph, and telephone lines. *See* Exec. Order No. 2604 (Apr. 28, 1917). During that war, wireless telegraphy "enabled each belligerent to tap the messages of the enemy." Bidwell, *supra*, at 165 (quoting statement of Col. W. Nicolai, former head of the Secret Service of the High Command of the German Army, *in* W. Nicolai, *The German Secret Service* 21 (1924)).

As noted in Part I, on May 21, 1940, President Roosevelt authorized warrantless electronic surveillance of persons suspected of subversive activities, including spying, against the United States. In addition, on December 8, 1941, the day after the attack on Pearl Harbor, President Roosevelt gave the Director of the FBI "temporary powers to direct all news censorship and to *control all other telecommunications traffic* in and out of the United States." Jack A. Gottschalk, *"Consistent with Security". . . . A History of American Military Press Censorship,* 5 Comm. & L. 35, 39 (1983) (emphasis added). *See* Memorandum for the Secretaries of War, Navy, State, and Treasury, the Postmaster General, and the Federal Communications Commission from Franklin D. Roosevelt (Dec. 8, 1941). President Roosevelt soon supplanted that temporary regime by establishing an office for conducting such electronic surveillance in accordance with the War Powers Act of 1941. *See* Pub. L. No. 77-354, § 303, 55 Stat. 838, 840-41 (Dec. 18, 1941); Gottschalk, 5 Comm. & L. at 40. The President's order gave the Government of the United States access to "communications by mail, cable, radio, or other means of transmission passing between the United States and any foreign country." *Id. See also* Exec. Order No. 8985, § 1, 6 Fed. Reg. 6625, 6625 (Dec. 19, 1941). In addition, the United States systematically listened surreptitiously to electronic communications as part of the war effort. *See* Dash, *Eavesdroppers* at 30. During World War II, signals intelligence assisted in, among other things, the destruction of the German U-boat fleet by the Allied naval forces, *see id.* at 27, and the war against Japan, *see* O'Toole, *supra*, at 32, 323-24. In general, signals intelligence "helped to shorten the war by perhaps two years, reduce the loss of life, and make inevitable an eventual Allied victory." Carl Boyd, *American Command of the Sea Through Carriers, Codes, and the Silent Service: World War II and Beyond* 27 (1995); *see also* Alvarez, *supra*, at 1 ("There can be little doubt that signals intelligence contributed significantly to the military defeat of the Axis."). Significantly, not only was wiretapping in World War II used "extensively by military intelligence and secret service personnel in combat areas abroad," but also "by the FBI and secret service in this country." Dash, *supra*, at 30.

In light of the long history of prior wartime practice, the NSA activities fit squarely within the sweeping terms of the AUMF. The use of signals intelligence to identify and pinpoint the enemy is a traditional component of wartime military operations—or, to use the terminology of *Hamdi*, a "fundamental and accepted . . . incident to war," 542 U.S. at 518 (plurality opinion)—employed to defeat the enemy and to prevent enemy attacks in the United States. Here, as in other conflicts, the enemy may use public communications networks, and some of the enemy may already be in the United States. Although those factors may be present in this conflict to a greater degree than in the past, neither is novel. Certainly, both factors were well known at the time Congress enacted the AUMF. Wartime interception of international communications made by the enemy thus should be understood, no less than the wartime detention at issue in *Hamdi*, as one of the basic methods of engaging and defeating the enemy that Congress authorized in approving "*all* necessary and appropriate force" that the President would need to defend the Nation. AUMF § 2(a) (emphasis added).

* * *

Accordingly, the President has the authority to conduct warrantless electronic surveillance against the declared enemy of the United States in a time of armed conflict. That authority derives from the Constitution, and is reinforced by the text and purpose of the AUMF, the nature of the threat posed by al Qaeda that Congress authorized the President to repel, and the long-established understanding that electronic surveillance is a fundamental incident of the use of military force. The President's power in authorizing the NSA activities is at its zenith because he has acted "pursuant to an express or implied authorization of Congress." *Youngstown*, 343 U.S. at 635 (Jackson, J., concurring).

III. THE NSA ACTIVITIES ARE CONSISTENT WITH THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

The President's exercise of his constitutional authority to conduct warrantless wartime electronic surveillance of the enemy, as confirmed and supplemented by statute in the AUMF, is fully consistent with the requirements of the Foreign Intelligence Surveillance Act ("FISA").[5] FISA is a critically important tool in the War on Terror. The United States makes full use of the authorities available under FISA to gather foreign intelligence information, including authorities to intercept communications, conduct physical searches, and install and use pen registers and trap and trace devices. While FISA establishes certain procedures that must be followed for these authorities to be used (procedures that usually involve applying for and obtaining an order from a special court), FISA also expressly contemplates that a later legislative enactment could

[5] To avoid revealing details about the operation of the program, it is assumed for purposes of this paper that the activities described by the President constitute "electronic surveillance," as defined by FISA, 50 U.S.C. § 1801(f).

authorize electronic surveillance outside the procedures set forth in FISA itself. The AUMF constitutes precisely such an enactment. To the extent there is any ambiguity on this point, the canon of constitutional avoidance requires that such ambiguity be resolved in favor of the President's authority to conduct the communications intelligence activities he has described. Finally, if FISA could not be read to allow the President to authorize the NSA activities during the current congressionally authorized armed conflict with al Qaeda, FISA would be unconstitutional as applied in this narrow context.

A. THE REQUIREMENTS OF FISA

FISA was enacted in 1978 to regulate "electronic surveillance," particularly when conducted to obtain "foreign intelligence information," as those terms are defined in section 101 of FISA, 50 U.S.C. § 1801. As a general matter, the statute requires that the Attorney General approve an application for an order from a special court composed of Article III judges and created by FISA—the Foreign Intelligence Surveillance Court ("FISC"). *See* 50 U.S.C. §§ 1803-1804. The application must demonstrate, among other things, that there is probable cause to believe that the target is a foreign power or an agent of a foreign power. *See id.* § 1805(a)(3)(A). It must also contain a certification from the Assistant to the President for National Security Affairs or an officer of the United States appointed by the President with the advice and consent of the Senate and having responsibilities in the area of national security or defense that the information sought is foreign intelligence information and cannot reasonably be obtained by normal investigative means. *See id.* § 1804(a)(7). FISA further requires the Government to state the means that it proposes to use to obtain the information and the basis for its belief that the facilities at which the surveillance will be directed are being used or are about to be used by a foreign power or an agent of a foreign power. *See id.* § 1804(a)(4), (a)(8).

FISA was the first congressional measure that sought to impose restrictions on the Executive Branch's authority to engage in electronic surveillance for foreign intelligence purposes, an authority that, as noted above, had been repeatedly recognized by the federal courts. *See* Americo R. Cinquegrana, *The Walls (and Wires) Have Ears: The Background and First Ten Years of the Foreign Intelligence Surveillance Act of 1978*, 137 U. Penn. L. Rev. 793, 810 (1989) (stating that the "status of the President's inherent authority" to conduct surveillance "formed the core of subsequent legislative deliberations" leading to the enactment of FISA). To that end, FISA modified a provision in Title III that previously had disclaimed any intent to have laws governing wiretapping interfere with the President's constitutional authority to gather foreign intelligence. Prior to the passage of FISA, section 2511(3) of title 18 had stated that "[n]othing contained in this chapter or in section 605 of the Communications Act of 1934 . . . shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities." 18 U.S.C. § 2511(3) (1970). FISA replaced that provision with an important, though more limited, preservation of authority for the President. *See* Pub. L. No. 95-511, § 201(b), (c), 92 Stat. 1783, 1797 (1978), codified at 18 U.S.C. § 2511(2)(f) (West Supp. 2005) (carving out from statutory regulation only the acquisition of intelligence information from "international or foreign communications" and "foreign intelligence activities . . . involving a foreign electronic communications system" as long as they are accomplished "utilizing a means other than electronic surveillance as defined in section 101" of FISA). Congress also defined "electronic surveillance," 50 U.S.C. § 1801(f), carefully and somewhat narrowly.[6]

In addition, Congress addressed, to some degree, the manner in which FISA might apply after a formal declaration of war by expressly allowing warrantless surveillance for a period of fifteen days following such a declaration. Section 111 of FISA allows the President to "authorize electronic surveillance without a court order under this subchapter to acquire foreign intelligence information for a period not to exceed fifteen calendar days following a declaration of war by the Congress." 50 U.S.C. § 1811.

The legislative history of FISA shows that Congress understood it was legislating on fragile constitutional ground and was pressing or even exceeding constitutional limits in regulating the President's authority in the field of foreign intelligence. The final House Conference Report, for example, recognized that the statute's restrictions might well impermissibly infringe on the President's constitutional powers. That report includes the extraordinary acknowledgment that "[t]he conferees agree that the establishment by this act of exclusive means by which the President may conduct electronic surveillance does not foreclose a different decision by the Supreme Court." H.R. Conf. Rep. No. 95-1720, at 35, *reprinted in* 1978 U.S.C.C.A.N. 4048, 4064. But, invoking Justice Jackson's concurrence in the *Steel Seizure* case, the Conference Report explained that Congress intended in FISA to exert whatever power Congress constitutionally had over the subject matter to restrict foreign intelligence surveillance and to leave the President solely with whatever inherent constitutional authority he might be able to invoke against Congress's express wishes. *Id.* The Report thus explains that "[t]he intent of the conferees is to apply the standard set forth in Justice Jackson's concurring opinion in the Steel Seizure Case: 'When a President takes measures incompatible with the express or implied will of Congress, his power is at the lowest ebb, for then he can rely only upon his own constitutional power minus any constitutional power of Congress over the matter.'" *Id.* (quoting *Youngstown Sheet & Tube Co.* v. *Sawyer,* 343 U.S. 579, 637 (1952) (Jackson, J., concurring)); *see also* S. Rep. No. 95-604, at 64, *reprinted in* 1978 U.S.C.C.A.N. at 3966 (same); *see generally* Elizabeth B. Bazen et al., Congressional Research Service, *Re: Presidential Authority to Conduct Warrantless Electronic Surveillance to Gather Foreign Intelligence Information* 28-29 (Jan. 5, 2006). It is significant, however, that Congress did not decide conclusively to continue to push the boundaries of its constitutional authority in wartime. Instead, Congress reserved the question of the appropriate procedures to regulate electronic surveillance in time of war, and established a fifteen-day period during which the President would be permitted to engage in electronic surveillance without complying with FISA's express procedures and during which Congress would have the opportunity to revisit the issue. *See* 50 U.S.C. § 1811; H.R. Conf. Rep. No. 95-1720, at 34, *reprinted in* 1978 U.S.C.C.A.N. at 4063 (noting that the purpose of the fifteen-day period following a declaration of war in section 111 of FISA was to "allow time for consideration of any amendment to this act that may be appropriate during a wartime emergency").

---

[6] FISA's legislative history reveals that these provisions were intended to exclude certain intelligence activities conducted by the National Security Agency from the coverage of FISA. According to the report of the Senate Judiciary Committee on FISA, "this provision [referencing what became the first part of section 2511(2)(f)] is designed to make clear that the legislation does not deal with international signals intelligence activities as currently engaged in by the National Security Agency and electronic surveillance conducted outside the United States." S. Rep. No. 95-604, at 64 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3965. The legislative history also makes clear that the definition of "electronic surveillance" was crafted for the same reason. *See id.* at 33-34, 1978 U.S.C.C.A.N. at 3934-36. FISA thereby "adopts the view expressed by the Attorney General during the hearings that enacting statutory controls to regulate the National Security Agency and the surveillance of Americans abroad raises problems best left to separate legislation." *Id.* at 64, 1978 U.S.C.C.A.N. at 3965. Such legislation placing limitations on traditional NSA activities was drafted, but never passed. *See* National Intelligence Reorganization and Reform Act of 1978: Hearings Before the Senate Select Committee on Intelligence, 95th Cong., 2d Sess. 999-1007 (1978) (text of unenacted legislation). And Congress understood that the NSA surveillance that it intended categorically to exclude from FISA could include the monitoring of international communications into or out of the United States of U.S. citizens. The report specifically referred to the Church Committee report for its description of the NSA's activities, S. Rep. No. 95-604, at 64 n.63, 1978 U.S.C.C.A.N. at 3965-66 n.63, which stated that "the NSA intercepts messages passing over international lines of communication, some of which have one terminal within the United States. Traveling over these lines of communication, especially those with one terminal in the United States, are messages of Americans . . . ." S. Rep. 94-755, at Book II, 308 (1976). Congress's understanding in the legislative history of FISA that such communications could be intercepted outside FISA procedures is notable.

B. FISA CONTEMPLATES AND ALLOWS SURVEILLANCE AUTHORIZED "BY STATUTE"

Congress did not attempt through FISA to prohibit the Executive Branch from using electronic surveillance. Instead, Congress acted to bring the exercise of that power under more stringent congressional control. *See, e.g.*, H. Conf. Rep. No. 95-1720, at 32, *reprinted in* 1978 U.S.C.C.A.N. 4048, 4064. Congress therefore enacted a regime intended to supplant the President's reliance on his own constitutional authority. Consistent with this overriding purpose of bringing the use of electronic surveillance under *congressional* control and with the commonsense notion that the Congress that enacted FISA could not bind future Congresses, FISA expressly contemplates that the Executive Branch may conduct electronic surveillance outside FISA's express procedures if and when a subsequent statute authorizes such surveillance.

Thus, section 109 of FISA prohibits any person from intentionally "engag[ing] . . . in electronic surveillance under color of law *except as authorized by statute*." 50 U.S.C. § 1809(a)(1) (emphasis added). Because FISA's prohibitory provision broadly exempts surveillance "authorized by statute," the provision demonstrates that Congress did not attempt to regulate through FISA electronic surveillance authorized by Congress through a subsequent enactment. The use of the term "statute" here is significant because it strongly suggests that *any* subsequent authorizing statute, not merely one that amends FISA itself, could legitimately authorize surveillance outside FISA's standard procedural requirements. *Compare* 18 U.S.C. § 2511(1) ("Except as otherwise specifically provided *in this chapter* any person who—(a) intentionally intercepts . . . any wire, oral, or electronic communication[] . . . shall be punished . . . .") (emphasis added); *id.* § 2511(2)(e) (providing a defense to liability to individuals "conduct[ing] electronic surveillance, . . . as authorized by *that Act [FISA]*") (emphasis added). In enacting FISA, therefore, Congress contemplated the possibility that the President might be permitted to conduct electronic surveillance pursuant to a later-enacted statute that did not incorporate all of the procedural requirements set forth in FISA or that did not expressly amend FISA itself.

To be sure, the scope of this exception is rendered less clear by the conforming amendments that FISA made to chapter 119 of title 18—the portion of the criminal code that provides the mechanism for obtaining wiretaps for law enforcement purposes. Before FISA was enacted, chapter 119 made it a criminal offense for any person to intercept a communication except as specifically provided in that chapter. *See* 18 U.S.C. § 2511(1)(a), (4)(a). Section 201(b) of FISA amended that chapter to provide an exception from criminal liability for activities conducted pursuant to FISA. Specifically, FISA added 18 U.S.C. § 2511(2)(e), which provides that it is not unlawful for "an officer, employee, or agent of the United States . . . to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act." *Id.* § 2511(2)(e). Similarly, section 201(b) of FISA amended chapter 119 to provide that "procedures in this chapter [or chapter 121 (addressing access to stored wire and electronic communications and customer records)] and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire, oral, and electronic communications may be conducted." *Id.* § 2511(2)(f) (West Supp. 2005).[7]

The amendments that section 201(b) of FISA made to title 18 are fully consistent, however, with the conclusion that FISA contemplates that a subsequent statute could authorize electronic surveillance outside FISA's express procedural requirements. Section 2511(2)(e) of title 18, which provides that it is "not unlawful" for an officer of the United States to conduct electronic surveillance "as authorized by" FISA, is best understood as a safe-harbor provision. Because of section 109, the protection offered by section 2511(2)(e) for surveillance "authorized by" FISA extends to surveillance that is authorized by any other statute and therefore excepted from the prohibition of section 109. In any event, the purpose of section 2511(2)(e) is merely to make explicit what would already have been implicit—that those authorized by statute to engage in particular surveillance do not act unlawfully when they conduct such surveillance. Thus, even if that provision had not been enacted, an officer conducting surveillance authorized by statute (whether FISA or some other law) could not reasonably have been thought to be violating Title III. Similarly, section 2511(2)(e) cannot be read to require a result that would be manifestly unreasonable—exposing a federal officer to criminal liability for engaging in surveillance authorized by statute, merely because the authorizing statute happens not to be FISA itself.

Nor could 18 U.S.C. § 2511(2)(f), which provides that the "procedures in this chapter . . . and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance . . . may be conducted," have been intended to trump the commonsense approach of section 109 and preclude a subsequent Congress from authorizing the President to engage in electronic surveillance through a statute other than FISA, using procedures other than those outlined in FISA or chapter 119 of title 18. The legislative history of section 2511(2)(f) clearly indicates an intent to prevent the President from engaging in surveillance except as

[7] The bracketed portion was added in 1986 amendments to section 2511(2)(f). *See* Pub. L. No. 99-508 § 101(b)(3), 100 Stat. 1848, 1850.

authorized by Congress, *see* H.R. Conf. Rep. No. 95-1720, at 32, *reprinted in* 1978 U.S.C.C.A.N. 4048, 4064, which explains why section 2511(2)(f) set forth all then-existing statutory restrictions on electronic surveillance. Section 2511(2)(f)'s reference to "exclusive means" reflected the state of statutory authority for electronic surveillance in 1978 and cautioned the President not to engage in electronic surveillance outside congressionally sanctioned parameters. It is implausible to think that, in attempting to limit the *President's* authority, Congress also limited its own future authority by barring subsequent Congresses from authorizing the Executive to engage in surveillance in ways not specifically enumerated in FISA or chapter 119, or by requiring a subsequent Congress specifically to amend FISA and section 2511(2)(f). There would be a serious question as to whether the Ninety-Fifth Congress could have so tied the hands of its successors. *See, e.g.*, *Fletcher v. Peck*, 10 U.S. (6 Cranch) 87, 135 (1810) (noting that "one legislature cannot abridge the powers of a succeeding legislature"); *Reichelderfer v. Quinn*, 287 U.S. 315, 318 (1932) ("[T]he will of a particular Congress . . . does not impose itself upon those to follow in succeeding years"); *Lockhart v. United States*, 126 S. Ct. 699, 703 (2005) (Scalia, J., concurring) (collecting precedent); 1 W. Blackstone, Commentaries on the Laws of England 90 (1765) ("Acts of parliament derogatory from the power of subsequent parliaments bind not"). In the absence of a clear statement to the contrary, it cannot be presumed that Congress attempted to abnegate its own authority in such a way.

Far from a clear statement of congressional intent to bind itself, there are indications that section 2511(2)(f) cannot be interpreted as requiring that *all* electronic surveillance and domestic interception be conducted under FISA's enumerated procedures or those of chapter 119 of title 18 until and unless those provisions are repealed or amended. Even when section 2511(2)(f) was enacted (and no subsequent authorizing statute existed), it could not reasonably be read to preclude all electronic surveillance conducted outside the procedures of FISA or chapter 119 of title 18. In 1978, use of a pen register or trap and trace device constituted electronic surveillance as defined by FISA. *See* 50 U.S.C. §§ 1801(f), (n). Title I of FISA provided procedures for obtaining court authorization for the use of pen registers to obtain foreign intelligence information. But the Supreme Court had, just prior to the enactment of FISA, held that chapter 119 of title 18 did not govern the use of pen registers. *See United States v. New York Tel. Co.*, 434 U.S. 159, 165-68 (1977). Thus, if section 2511(2)(f) were to be read to permit of no exceptions, the use of pen registers for purposes other than to collect foreign intelligence information would have been unlawful because such use would not have been authorized by the "exclusive" procedures of section 2511(2)(f), *i.e.*, FISA and chapter 119. But no court has held that pen registers could not be authorized outside the foreign intelligence context. Indeed, FISA appears to have recognized this issue by providing a defense to liability for any official who engages in electronic surveillance under a search warrant or court order. *See* 50 U.S.C. § 1809(b). (The practice when FISA was enacted was for law enforcement officers to obtain search warrants under the Federal Rules of Criminal Procedure authorizing the installation and use of pen registers. *See S. 1667, A Bill to Amend Title 18, United States Code, with Respect to the Interception of Certain Communications, Other Forms of Surveillance, and for Other Purposes: Hearing Before the Subcomm. On Patents, Copyrights and Trademarks of the Senate*

Comm. on the Judiciary, 99th Cong. 57 (1985) (prepared statement of James Knapp, Deputy Assistant Attorney General, Criminal Division)).[8]

In addition, section 2511(2)(a)(ii) authorizes telecommunications providers to assist officers of the Government engaged in electronic surveillance when the Attorney General certifies that "no warrant or court order is required by law [and] that all statutory requirements have been met." 18 U.S.C. § 2511(2)(a)(ii).[9] If the Attorney General can certify, in good faith, that the requirements of a subsequent statute authorizing electronic surveillance are met, service providers are affirmatively and expressly authorized to assist the Government. Although FISA does allow the Government to proceed without a court order in several situations, *see* 50 U.S.C. § 1805(f) (emergencies); *id.* § 1802 (certain communications between foreign governments), this provision specifically lists only Title III's emergency provision but speaks generally to Attorney General certification. That reference to Attorney General certification is consistent with the historical practice in which Presidents have delegated to the Attorney General authority to approve warrantless surveillance for foreign intelligence purposes. *See, e.g.*, *United States v. United States District Court,* 444 F.2d 651, 669-71 (6th Cir. 1971) (reproducing as an appendix memoranda from Presidents Roosevelt, Truman, and Johnson). Section 2511(2)(a)(ii) thus suggests that telecommunications providers can be authorized to assist with warrantless electronic surveillance when such surveillance is authorized by law outside FISA.

In sum, by expressly and broadly excepting from its prohibition electronic surveillance undertaken "as authorized by statute," section 109 of FISA permits an exception to the "procedures" of FISA referred to in 18 U.S.C. § 2511(2)(f) where authorized by another statute, even if the other authorizing statute does not specifically amend section 2511(2)(f).

C. THE AUMF IS A "STATUTE" AUTHORIZING SURVEILLANCE OUTSIDE THE CONFINES OF FISA

The AUMF qualifies as a "statute" authorizing electronic surveillance within the meaning of section 109 of FISA.

First, because the term "statute" historically has been given broad meaning, the phrase "authorized by statute" in section 109 of FISA must be read to include joint resolutions such as the AUMF. *See American Fed'n of Labor v. Watson*, 327 U. S. 582, 592-93 (1946) (finding the term "statute" as used in 28 U.S.C. § 380 to mean "a compendious summary of various enactments, by whatever method they may be adopted, to which a State gives her sanction"); Black's Law Dictionary 1410 (6th ed. 1990) (defining "statute" broadly to include any "formal written enactment of a legislative body," and stating that the term is used "to designate the legislatively created laws in contradistinction to court decided or unwritten laws"). It is thus of no significance to this analysis that the AUMF was enacted as a joint resolution rather than a bill. *See, e.g., Ann Arbor R.R. Co. v. United States*, 281 U.S. 658, 666 (1930) (joint resolutions are to be construed by applying "the rules applicable to legislation in general"); *United States ex rel. Levey v. Stockslager*, 129 U.S. 470, 475 (1889) (joint resolution had "all the characteristics and effects" of statute that it suspended); *Padilla ex rel. Newman v. Bush*, 233 F. Supp. 2d 564, 598 (S.D.N.Y 2002) (in analyzing the AUMF, finding that there is "no relevant constitutional difference between a bill and a joint resolution"), *rev'd sub nom. on other grounds, Rumsfeld v. Padilla*, 352 F.3d 695 (2d Cir. 2003), *rev'd*, 542 U.S. 426 (2004); *see also* Letter for the Hon. John Conyers, Jr., U.S. House of Representatives, from Prof. Laurence H. Tribe at 3 (Jan. 6, 2006) (term "statute" in section 109 of FISA "of course encompasses a joint resolution presented to and signed by the President").

---

[8] Alternatively, section 109(b) may be read to constitute a "procedure" in FISA or to incorporate procedures from sources other than FISA (such as the Federal Rules of Criminal Procedure or state court procedures), and in that way to satisfy section 2511(2)(f). But if section 109(b)'s defense can be so read, section 109(a) should also be read to constitute a procedure or incorporate procedures not expressly enumerated in FISA.

[9] Section 2511(2)(a)(ii) states:

> Notwithstanding any other law, providers of wire or electronic communication service, . . . are authorized by law to provide information, facilities, or technical assistance to persons authorized by law to intercept . . . communications or to conduct electronic surveillance, as defined [by FISA], if such provider . . . has been provided with . . . a certification in writing by [specified persons proceeding under Title III's emergency provision] or the Attorney General of the United States that no warrant or court order is required by law, that all statutory requirements have been met, and that the specific assistance is required.

Second, the longstanding history of communications intelligence as a fundamental incident of the use of force and the Supreme Court's decision in *Hamdi v. Rumsfeld* strongly suggest that the AUMF satisfies the requirement of section 109 of FISA for statutory authorization of electronic surveillance. As explained above, it is not necessary to demarcate the outer limits of the AUMF to conclude that it encompasses electronic surveillance targeted at the enemy. Just as a majority of the Court concluded in *Hamdi* that the AUMF authorizes detention of U.S. citizens who are enemy combatants without expressly mentioning the President's long-recognized power to detain, so too does it authorize the use of electronic surveillance without specifically mentioning the President's equally long-recognized power to engage in communications intelligence targeted at the enemy. And just as the AUMF satisfies the requirement in 18 U.S.C. § 4001(a) that no U.S. citizen be detained "except pursuant to an Act of Congress," so too does it satisfy section 109's requirement for statutory authorization of electronic surveillance.[10] In authorizing the President's use of force in response to the September 11th attacks, Congress did not need to comb through the United States Code looking for those restrictions that it had placed on national security operations during times of peace and designate with specificity each traditional tool of military force that it sought to authorize the President to use. There is no historical precedent for such a requirement: authorizations to use

[10] It might be argued that Congress dealt more comprehensively with electronic surveillance in FISA than it did with detention in 18 U.S.C. § 4001(a). Thus, although Congress prohibited detention "except pursuant to an Act of Congress," it combined the analogous prohibition in FISA (section 109(a)) with section 2511(2)(f)'s exclusivity provision. *See* Letter to the Hon. Bill Frist, Majority Leader, U.S. Senate, from Professor Curtis A. Bradley *et al.* at 5 n.6 (Jan. 9, 2006) (noting that section 4001(a) does not "attempt[] to create an exclusive mechanism for detention"). On closer examination, however, it is evident that Congress has regulated detention far more meticulously than these arguments suggest. Detention is the topic of much of the Criminal Code, as well as a variety of other statutes, including those providing for civil commitment of the mentally ill and confinement of alien terrorists. The existence of these statutes and accompanying extensive procedural safeguards, combined with the substantial constitutional issues inherent in detention, *see, e.g., Hamdi*, 542 U.S. at 574-75 (Scalia, J., dissenting), refute any such argument.

military force traditionally have been couched in general language. Indeed, prior administrations have interpreted joint resolutions declaring war and authorizing the use of military force to authorize expansive collection of communications into and out of the United States.[11]

Moreover, crucial to the Framers' decision to vest the President with primary constitutional authority to defend the Nation from foreign attack is the fact that the Executive can act quickly, decisively, and flexibly as needed. For Congress to have a role in that process, it must be able to act with similar speed, either to lend its support to, or to signal its disagreement with, proposed military action. Yet the need for prompt decisionmaking in the wake of a devastating attack on the United States is fundamentally inconsistent with the notion that to do so Congress must legislate at a level of detail more in keeping with a peacetime budget reconciliation bill. In emergency situations, Congress must be able to use broad language that effectively sanctions the President's use of the core incidents of military force. That is precisely what Congress did when it passed the AUMF on September 14, 2001—just three days after the deadly attacks on America. The Capitol had been evacuated on September 11th, and Congress was meeting in scattered locations. As an account emerged of who might be responsible for these attacks, Congress acted quickly to authorize the President to use "all necessary and appropriate force" against the enemy that he determines was involved in the September 11th attacks. Under these circumstances, it would be unreasonable and wholly impractical to demand that Congress specifically amend FISA in order to assist the President in defending the Nation. Such specificity would also have been self-defeating because it would have apprised our adversaries of some of our most sensitive methods of intelligence gathering.[12]

Section 111 of FISA, 50 U.S.C. § 1811, which authorizes the President, "[n]otwithstanding any other law," to conduct "electronic surveillance without a court order under this subchapter to acquire foreign intelligence information for a period not to exceed fifteen calendar days following a declaration of war by Congress," does not require a different reading of the AUMF. *See also id.* § 1844 (same provision for pen registers); *id.* § 1829 (same provision for physical searches). Section 111 cannot reasonably be read as Congress's final word on electronic surveillance during wartime, thus permanently limiting the President in all circumstances to a mere fifteen days of warrantless military intelligence gathering targeted at the enemy following a declaration of war. Rather, section 111 represents Congress's recognition that it would likely have to return to the subject and provide additional authorization to conduct warrantless electronic surveillance outside FISA during time of war. The Conference Report explicitly stated the conferees' "inten[t] that this [fifteen-day] period will allow time for consideration of any amendment to this act that may be appropriate during a wartime emergency." H.R. Conf. Rep. No. 95-1720, at 34, *reprinted in* 1978 U.S.C.C.A.N. at 4063. Congress enacted section 111 so that the President could conduct warrantless surveillance while Congress considered supplemental wartime legislation.

---

[11] As noted above, in intercepting communications, President Wilson relied on his constitutional authority and the joint resolution declaring war and authorizing the use of military force, which, as relevant here, provided "that the President [is] authorized and directed to employ the entire naval and military forces of the United States and the resources of the Government to carry on war against the Imperial German Government; and to bring the conflict to a successful termination all of the resources of the country are hereby pledged by the Congress of the United States." Joint Resolution of Apr. 6, 1917, ch. 1, 40 Stat. 1. The authorization did not explicitly mention interception of communications.

[12] Some have suggested that the Administration declined to seek a specific amendment to FISA allowing the NSA activities "because it was advised that Congress would reject such an amendment," Letter to the Hon. Bill Frist, Majority Leader, U.S. Senate, from Professor Curtis A. Bradley *et al.* 4 & n.4 (Jan. 9, 2005), and they have quoted in support of that assertion the Attorney General's statement that certain Members of Congress advised the Administration that legislative relief "would be difficult, if not impossible." *Id.* at 4 n.4. As the Attorney General subsequently indicated, however, the difficulty with such specific legislation was that it could not be enacted "without compromising the program." *See* Remarks by Homeland Security Secretary Chertoff and Attorney General Gonzales on the USA PATRIOT Act (Dec. 21, 2005), *available at* http://www.dhs.gov/dhspublic/display?content=5285.

Nothing in the terms of section 111 disables Congress from authorizing such electronic surveillance as a traditional incident of war through a broad, conflict-specific authorization for the use of military force, such as the AUMF. Although the legislative history of section 111 indicates that in 1978 some Members of Congress believed that any such authorization would come in the form of a particularized amendment to FISA itself, section 111 does not require that result. Nor could the Ninety-Fifth Congress tie the hands of a subsequent Congress in this way, at least in the absence of far clearer statutory language expressly requiring that result. *See supra*, pp. 21-22; *compare, e.g.*, War Powers Resolution, § 8, 50 U.S.C. § 1547(a) ("Authority to introduce United States Armed Forces into hostilities . . . shall not be inferred . . . from any provision of law . . . unless such provision specifically authorizes [such] introduction . . . and states that it is intended to constitute specific statutory authorization within the meaning of this chapter."); 10 U.S.C. § 401 (stating that any other provision of law providing assistance to foreign countries to detect and clear landmines shall be subject to specific limitations and may be construed as superseding such limitations "only if, and to the extent that, such provision specifically refers to this section and specifically identifies the provision of this section that is to be considered superseded or otherwise inapplicable"). An interpretation of section 111 that would disable Congress from authorizing broader electronic surveillance in that form can be reconciled neither with the purposes of section 111 nor with the well-established proposition that "one legislature cannot abridge the powers of a succeeding legislature." *Fletcher v. Peck*, 10 U.S. (6 Cranch) at 135; *see supra* Part II.B. For these reasons, the better interpretation is that section 111 was not intended to, and did not, foreclose Congress from using the AUMF as the legal vehicle for supplementing the President's existing authority under FISA in the battle against al Qaeda.

The contrary interpretation of section 111 also ignores the important differences between a formal declaration of war and a resolution such as the AUMF. As a historical matter, a formal declaration of war was no longer than a sentence, and thus Congress would not expect a declaration of war to outline the extent to which Congress authorized the President to engage in various incidents of waging war. Authorizations for the use of military force, by contrast, are typically more detailed and are made for the *specific purpose* of reciting the manner in which Congress has authorized the President to act. Thus, Congress could reasonably expect that an authorization for the use of military force would address the issue of wartime surveillance, while a declaration of war would not. Here, the AUMF declares that the Nation faces "an unusual and extraordinary threat," acknowledges that "the President has authority under the Constitution to take action to deter and prevent acts of international terrorism against the United States," and provides that the President is authorized "to use all necessary and appropriate force" against those "he determines" are linked to the September 11th attacks. AUMF pmbl., § 2. This sweeping language goes far beyond the bare terms of a declaration of war. *Compare, e.g.*, Act of Apr. 25, 1898, ch. 189, 30 Stat. 364 ("First. That war be, and the same is hereby declared to exist . . . between the United States of America and the Kingdom of Spain.").

Although legislation that has included a declaration of war has often also included an authorization of the President to use force, these provisions are separate and need not be combined in a single statute. *See, e.g., id.* ("Second. That the President of the United States be, and he hereby is, directed and empowered to use the entire land and naval forces of the United States, and to call into the actual service of the United States the militia of the several states, *to such extent as may be necessary to carry this Act into effect.*") (emphasis added). Moreover, declarations of war have legal significance independent of any additional authorization of force that might follow. *See, e.g.*, Louis Henkin, *Foreign Affairs and the U.S. Constitution* 75 (2d ed. 1996) (explaining that a formal state of war has various legal effects, such as terminating diplomatic relations, and abrogating or suspending treaty obligations and international law rights and duties); *see also id.* at 370 n.65 (speculating that one reason to fight an undeclared war would be to "avoid the traditional consequences of declared war on relations with third nations or even . . . belligerents").

In addition, section 111 does not cover the vast majority of modern military conflicts. The last declared war was World War II. Indeed, the most recent conflict prior to the passage of FISA, Vietnam, was fought without a formal declaration of war. In addition, the War Powers Resolution, enacted less than five years before FISA, clearly recognizes the distinctions between formal declarations of war and authorizations of force and demonstrates that, if Congress had wanted to include such authorizations in section 111, it knew how to do so. *See, e.g.*, 50 U.S.C. § 1544(b) (attempting to impose certain consequences 60 days after reporting the initiation of hostilities to Congress "unless the Congress . . . has declared war *or has enacted a specific authorization for such use*" of military force) (emphasis added). It is possible that, in enacting section 111, Congress intended to make no provision for even the temporary use of electronic surveillance without a court order for what had become the legal regime for most military conflicts. A better reading, however, is that Congress assumed that such a default provision would be unnecessary because, if it had acted through an authorization for the use of military force, the more detailed provisions of that authorization would resolve the extent to which Congress would attempt to authorize, or withhold authorization for, the use of electronic surveillance.[13]

---

[13] Some have pointed to the specific amendments to FISA that Congress made shortly after September 11th in the USA PATRIOT Act, Pub. L. No. 107-56, §§ 204, 218, 115 Stat. 272, 281, 291 (2001), to argue that Congress did not contemplate electronic surveillance outside the parameters of FISA. *See* Memorandum for Members of the House Permanent Select Comm. on Intel. from Jeffrey H. Smith, *Re: Legal Authorities Regarding Warrantless Surveillance of U.S. Persons* 6-7 (Jan. 3, 2006). The USA PATRIOT Act amendments, however, do not justify giving the AUMF an unnaturally narrow reading. The USA PATRIOT Act amendments made important corrections in the general application of FISA; they were not intended to define the precise incidents of military force that would be available to the President in prosecuting the current armed conflict against al Qaeda and its allies. Many removed long-standing impediments to the effectiveness of FISA that had contributed to the

*   *   *

The broad text of the AUMF, the authoritative interpretation that the Supreme Court gave it in *Hamdi*, and the circumstances in which it was passed demonstrate that the AUMF is a statute authorizing electronic surveillance under section 109 of FISA. When the President authorizes electronic surveillance against the enemy pursuant to the AUMF, he is therefore acting at the height of his authority under *Youngstown*, 343 U.S. at 637 (Jackson, J., concurring).

D. THE CANON OF CONSTITUTIONAL AVOIDANCE REQUIRES RESOLVING IN FAVOR OF THE PRESIDENT'S AUTHORITY ANY AMBIGUITY ABOUT WHETHER FISA FORBIDS THE NSA ACTIVITIES

As explained above, the AUMF fully authorizes the NSA activities. Because FISA contemplates the possibility that subsequent statutes could authorize electronic surveillance without requiring FISA's standard procedures, the NSA activities are also consistent with FISA and related provisions in title 18. Nevertheless, some might argue that sections 109 and 111 of FISA, along with section 2511(2)(f)'s "exclusivity" provision and section 2511(2)(e)'s liability exception for officers engaged in FISA-authorized surveillance, are best read to suggest that FISA requires that subsequent authorizing legislation specifically amend FISA in order to free the Executive from FISA's enumerated procedures. As detailed above, this is not the better reading of FISA. But even if these provisions were ambiguous, any doubt as to whether the AUMF and FISA should be understood to allow the President to make tactical military decisions to authorize surveillance outside the parameters of FISA must be resolved to avoid the serious constitutional questions that a contrary interpretation would raise.

It is well established that the first task of any interpreter faced with a statute that may present an unconstitutional infringement on the powers of the President is to determine whether the statute may be construed to avoid the constitutional difficulty. "[I]f an otherwise acceptable

---

maintenance of an unnecessary "wall" between foreign intelligence gathering and criminal law enforcement; others were technical clarifications. *See In re Sealed Case,* 310 F.3d 717, 725-30 (Foreign Int. Surv. Ct. Rev. 2002). The "wall" had been identified as a significant problem hampering the Government's efficient use of foreign intelligence information well before the September 11th attacks and in contexts unrelated to terrorism. *See, e.g., Final Report of the Attorney General's Review Team on the Handling of the Los Alamos National Laboratory Investigation* 710, 729, 732 (May 2000); General Accounting Office, *FBI Intelligence Investigations: Coordination Within Justice on Counterintelligence Criminal Matters Is Limited* (GAO-01-780) 3, 31 (July 2001). Finally, it is worth noting that Justice Souter made a similar argument in *Hamdi* that the USA PATRIOT Act all but compelled a narrow reading of the AUMF. *See* 542 U.S. at 551 ("It is very difficult to believe that the same Congress that carefully circumscribed Executive power over alien terrorists on home soil [in the USA PATRIOT Act] would not have meant to require the Government to justify clearly its detention of an American citizen held on home soil incommunicado."). Only Justice Ginsburg joined this opinion, and the position was rejected by a majority of Justices.

Nor do later amendments to FISA undermine the conclusion that the AUMF authorizes electronic surveillance outside the procedures of FISA. Three months after the enactment of the AUMF, Congress enacted certain "technical amendments" to FISA which, *inter alia*, extended the time during which the Attorney General may issue an emergency authorization of electronic surveillance from 24 to 72 hours. *See* Intelligence Authorization Act for Fiscal Year 2002, Pub. L. No. 107-108, § 314, 115 Stat. 1394, 1402 (2001). These modifications to FISA do not in any way undermine Congress's previous authorization in the AUMF for the President to engage in electronic surveillance outside the parameters of FISA in the specific context of the armed conflict with al Qaeda.

construction of a statute would raise serious constitutional problems, and where an alternative interpretation of the statute is 'fairly possible,' we are obligated to construe the statute to avoid such problems." *INS v. St. Cyr*, 533 U.S. 289, 299-300 (2001) (citations omitted); *Ashwander v. TVA*, 297 U.S. 288, 345-48 (1936) (Brandeis, J., concurring). Moreover, the canon of constitutional avoidance has particular importance in the realm of national security, where the President's constitutional authority is at its highest. *See Department of the Navy v. Egan*, 484 U.S. 518, 527, 530 (1988); William N. Eskridge, Jr., *Dynamic Statutory Interpretation* 325 (1994) (describing "[s]uper-strong rule against congressional interference with the President's authority over foreign affairs and national security"). Thus, courts and the Executive Branch typically construe a general statute, even one that is written in unqualified terms, to be implicitly limited so as not to infringe on the President's Commander in Chief powers.

Reading FISA to prohibit the NSA activities would raise two serious constitutional questions, both of which must be avoided if possible: (1) whether the signals intelligence collection the President determined was necessary to undertake is such a core exercise of Commander in Chief control over the Armed Forces during armed conflict that Congress cannot interfere with it at all and (2) whether the particular restrictions imposed by FISA are such that their application would impermissibly impede the President's exercise of his constitutionally assigned duties as Commander in Chief. Constitutional avoidance principles require interpreting FISA, at least in the context of the military conflict authorized by the AUMF, to avoid these questions, if "fairly possible." Even if Congress intended FISA to use the full extent of its constitutional authority to "occupy the field" of "electronic surveillance," as FISA used that term, during peacetime, the legislative history indicates that Congress had not reached a definitive conclusion about its regulation during wartime. *See* H.R. Conf. Rep. No. 95-1720, at 34, *reprinted in* 1978 U.S.C.C.A.N. at 4063 (noting that the purpose of the fifteen-day period following a declaration of war in section 111 of FISA was to "allow time for consideration of any amendment to this act that may be appropriate during a wartime emergency"). Therefore, it is not clear that Congress, in fact, intended to test the limits of its constitutional authority in the context of wartime electronic surveillance.

Whether Congress may interfere with the President's constitutional authority to collect foreign intelligence information through interception of communications reasonably believed to be linked to the enemy poses a difficult constitutional question. As explained in Part I, it had long been accepted at the time of FISA's enactment that the President has inherent constitutional authority to conduct warrantless electronic surveillance for foreign intelligence purposes. Congress recognized at the time that the enactment of a statute purporting to eliminate the President's ability, even during peacetime, to conduct warrantless electronic surveillance to collect foreign intelligence was near or perhaps beyond the limit of Congress's Article I powers. The NSA activities, however, involve signals intelligence performed in the midst of a congressionally authorized armed conflict undertaken to prevent further hostile attacks on the United States. The NSA activities lie at the very core of the Commander in Chief power, especially in light of the AUMF's explicit authorization for the President to take *all* necessary and appropriate military action to stop al Qaeda from striking again. The constitutional principles at stake here thus involve not merely the President's well-established inherent authority to conduct warrantless surveillance for foreign intelligence purposes during peacetime, but also the powers and duties expressly conferred on him as Commander in Chief by Article II.

Even outside the context of wartime surveillance of the enemy, the source and scope of Congress's power to restrict the President's inherent authority to conduct foreign intelligence surveillance is unclear. As explained above, the President's role as sole organ for the Nation in foreign affairs has long been recognized as carrying with it preeminent authority in the field of national security and foreign intelligence. The source of this authority traces to the Vesting Clause of Article II, which states that "[t]he executive Power shall be vested in a President of the United States of America." U.S. Const. art. II, § 1. The Vesting Clause "has long been held to confer on the President plenary authority to represent the United States and to pursue its interests outside the borders of the country, subject only to limits specifically set forth in the Constitution itself and to such statutory limitations as the Constitution permits Congress to impose by exercising one of its enumerated powers." *The President's Compliance with the "Timely Notification" Requirement of Section 501(b) of the National Security Act*, 10 Op. O.L.C. 159, 160-61 (1986) ("*Timely Notification Requirement Op.*").

Moreover, it is clear that some presidential authorities in this context are beyond Congress's ability to regulate. For example, as the Supreme Court explained in *Curtiss-Wright*, the President "*makes* treaties with the advice and consent of the Senate; but he alone negotiates. Into the field of negotiation the Senate cannot intrude; and Congress itself is powerless to invade it." 299 U.S. at 319. Similarly, President Washington established early in the history of the Republic the Executive's absolute authority to maintain the secrecy of negotiations with foreign powers, even against congressional efforts to secure information. *See id.* at 320-21. Recognizing presidential authority in this field, the Executive Branch has taken the position that "congressional legislation authorizing extraterritorial diplomatic and intelligence activities is superfluous, and . . . statutes infringing the President's inherent Article II authority would be unconstitutional." *Timely Notification Requirement Op.*, 10 Op. O.L.C. at 164.

There are certainly constitutional limits on Congress's ability to interfere with the President's power to conduct foreign intelligence searches, consistent with the Constitution, within the United States. As explained above, intelligence gathering is at the heart of executive functions. Since the time of the Founding it has been recognized that matters requiring secrecy—and intelligence in particular—are quintessentially executive functions. *See, e.g., The Federalist No. 64*, at 435 (John Jay) (Jacob E. Cooke ed. 1961) ("The convention have done well therefore in so disposing of the power of making treaties, that although the president must in forming them act by the advice and consent of the senate, yet he will be able to manage the business of intelligence in such manner as prudence may suggest."); *see also Timely Notification Requirement Op.*, 10 Op. O.L.C. at 165; *cf. New York Times Co. v. United States,* 403 U.S. 713, 729-30 (1971) (Stewart, J., concurring) ("[I]t is the constitutional duty of the Executive—as a matter of sovereign prerogative and not as a matter of law as the courts know law—through the promulgation and enforcement of executive regulations, to protect the confidentiality necessary to carry out its responsibilities in the field of international relations and national defense.").

Because Congress has rarely attempted to intrude in this area and because many of these questions are not susceptible to judicial review, there are few guideposts for determining exactly where the line defining the President's sphere of exclusive authority lies. Typically, if a statute is in danger of encroaching upon exclusive powers of the President, the courts apply the constitutional avoidance canon, if a construction avoiding the constitutional issue is "fairly possible." *See, e.g., Egan,* 484 U.S. at 527, 530. The only court that squarely has addressed the relative powers of Congress and the President in this field suggested that the balance tips decidedly in the President's favor. The Foreign Intelligence Surveillance Court of Review recently noted that all courts to have addressed the issue of the President's inherent authority have "held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information." *In re Sealed Case,* 310 F.3d 717, 742 (Foreign Intel. Surv. Ct. of Rev. 2002). On the basis of that unbroken line of precedent, the court "[took] for granted that the President does have that authority," and concluded that, "assuming that is so, FISA could not encroach on the President's constitutional power." *Id.*[14] Although the court did not provide extensive analysis, it is the only judicial statement on point, and it comes from the specialized appellate court created expressly to deal with foreign intelligence issues under FISA.

But the NSA activities are not simply exercises of the President's general foreign affairs powers. Rather, they are primarily an exercise of the President's authority as Commander in Chief during an armed conflict that Congress expressly has authorized the President to pursue. The NSA activities, moreover, have been undertaken specifically to prevent a renewed attack at the hands of an enemy that has already inflicted the single deadliest foreign attack in the Nation's history. The core of the Commander in Chief power is the authority to direct the Armed Forces in conducting a military campaign. Thus, the Supreme Court has made clear that the "President alone" is "constitutionally invested with the entire charge of hostile operations." *Hamilton v. Dillin,* 88 U.S. (21 Wall.) 73, 87 (1874); *The Federalist* No. 74, at 500 (Alexander Hamilton). "As commander-in-chief, [the President] is authorized to direct the movements of the naval and military forces placed by law at his command, and to employ them in the manner he may deem most effectual to harass and conquer and subdue the enemy." *Fleming v. Page,* 50 U.S. (9 How.) 603, 615 (1850). As Chief Justice Chase explained in 1866, although Congress has authority to legislate to support the prosecution of a war, Congress may not "*interfere[] with the command of the forces and the conduct of campaigns.* That power and duty belong to the President as commander-in-chief." *Ex parte Milligan,* 71 U.S. (4 Wall.) 2, 139 (1866) (Chase, C.J., concurring in judgment) (emphasis added).

The Executive Branch uniformly has construed the Commander in Chief and foreign affairs powers to grant the President authority that is beyond the ability of Congress to regulate. In 1860, Attorney General Black concluded that an act of Congress, if intended to constrain the President's discretion in assigning duties to an officer in the army, would be unconstitutional:

As commander-in-chief of the army it is your right to decide according to your

[14] In the past, other courts have declined to express a view on that issue one way or the other. *See, e.g., Butenko,* 494 F.2d at 601 ("We do not intimate, at this time, any view whatsoever as the proper resolution of the possible clash of the constitutional powers of the President and Congress.").

own judgment what officer shall perform any particular duty, and as the supreme executive magistrate you have the power of appointment. Congress could not, if it would, take away from the President, or in anywise diminish the authority conferred upon him by the Constitution.

Memorial of Captain Meigs, 9 Op. Att'y Gen. 462, 468 (1860). Attorney General Black went on to explain that, in his view, the statute involved there could probably be read as simply providing "a recommendation" that the President could decline to follow at his discretion. *Id.* at 469-70.[15]

Supreme Court precedent does not support claims of congressional authority over core military decisions during armed conflicts. In particular, the two decisions of the Supreme Court that address a conflict between asserted wartime powers of the Commander in Chief and congressional legislation and that resolve the conflict in favor of Congress—*Little v. Barreme*, 6 U.S. (2 Cranch) 170 (1804), and *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579 (1952)—are both distinguishable from the situation presented by the NSA activities in the conflict with al Qaeda. Neither supports the constitutionality of the restrictions in FISA as applied here.

Barreme involved a suit brought to recover a ship seized by an officer of the U.S. Navy on the high seas during the so-called "Quasi War" with France in 1799. The seizure had been based upon the officer's orders implementing an act of Congress suspending commerce between the United States and France and authorizing the seizure of American ships bound *to* a French port. The ship in question was suspected of sailing *from* a French port. The Supreme Court held that the orders given by the President could not authorize a seizure beyond the terms of the

[15] Executive practice recognizes, consistent with the Constitution, some congressional control over the Executive's decisions concerning the Armed Forces. *See, e.g.*, U.S. Const. art. I, § 8, cl. 12 (granting Congress power "to raise and support Armies"). But such examples have not involved congressional attempts to regulate the actual conduct of a military campaign, and there is no comparable textual support for such interference. For example, just before World War II, Attorney General Robert Jackson concluded that the Neutrality Act prohibited President Roosevelt from selling certain armed naval vessels and sending them to Great Britain. *See Acquisition of Naval and Air Bases in Exchange for Over-Age Destroyers*, 39 Op. Att'y Gen. 484, 496 (1940). Jackson's apparent conclusion that Congress could control the President's ability to transfer war material does not imply acceptance of direct congressional regulation of the Commander in Chief's control of the means and methods of engaging the enemy in conflict. Similarly, in *Youngstown Sheet & Tube Co. v. Sawyer*, the Truman Administration readily conceded that, if Congress had prohibited the seizure of steel mills by statute, Congress's action would have been controlling. *See* Brief for Petitioner at 150, *Youngstown*, 343 U.S. 579 (1952) (Nos. 744 and 745). This concession implies nothing concerning congressional control over the methods of engaging the enemy.

Likewise, the fact that the Executive Branch has, at times, sought congressional ratification after taking unilateral action in a wartime emergency does not reflect a concession that the Executive lacks authority in this area. A decision to seek congressional support can be prompted by many motivations, including a desire for political support. In modern times, several administrations have sought congressional authorization for the use of military force while preserving the ability to assert the unconstitutionality of the War Powers Resolution. *See, e.g.*, *Statement on Signing the Resolution Authorizing the Use of Military Force Against Iraq*, 1 Pub. Papers of George Bush 40 (1991) ("[M]y request for congressional support did not . . . constitute any change in the long-standing positions of the executive branch on either the President's constitutional authority to use the Armed Forces to defend vital U.S. interests or the constitutionality of the War Powers Resolution."). Moreover, many actions for which congressional support has been sought—such as President Lincoln's action in raising an Army in 1861—quite likely fall primarily under Congress's core Article I powers.

statute and therefore that the seizure of the ship not in fact bound *to* a French port was unlawful. *See* 6 U.S. at 177-78. Although some commentators have broadly characterized *Barreme* as standing for the proposition that Congress may restrict by statute the means by which the President can direct the Nation's Armed Forces to carry on a war, the Court's holding was limited in at least two significant ways. First, the operative section of the statute in question applied only to *American* merchant ships. *See id.* at 170 (quoting Act of February 9, 1799). Thus, the Court simply had no occasion to rule on whether, even in the limited and peculiar circumstances of the Quasi War, Congress could have placed some restriction on the orders the Commander in Chief could issue concerning direct engagements with enemy forces. Second, it is significant that the statute in *Barreme* was cast expressly, not as a limitation on the conduct of warfare by the President, but rather as regulation of a subject within the core of Congress's enumerated powers under Article I—the regulation of foreign commerce. *See* U.S. Const., art. I, § 8, cl. 3. The basis of Congress's authority to act was therefore clearer in *Barreme* than it is here.

Youngstown involved an effort by the President—in the face of a threatened work stoppage—to seize and to run steel mills. Congress had expressly considered the possibility of giving the President power to effect such a seizure during national emergencies. It rejected that option, however, instead providing different mechanisms for resolving labor disputes and mechanisms for seizing industries to ensure production vital to national defense.

For the Court, the connection between the seizure and the core Commander in Chief function of commanding the Armed Forces was too attenuated. The Court pointed out that the case did not involve authority over "day-to-day fighting in a theater of war." *Id.* at 587. Instead, it involved a dramatic extension of the President's authority over military operations to exercise control over an industry that was vital for producing equipment needed overseas. Justice Jackson's concurring opinion also reveals a concern for what might be termed foreign-to-domestic presidential bootstrapping. The United States became involved in the Korean conflict through President Truman's unilateral decision to commit troops to the defense of South Korea. The President then claimed authority, based upon this foreign conflict, to extend presidential control into vast sectors of the domestic economy. Justice Jackson expressed "alarm[]" at a theory under which "a President whose conduct of foreign affairs is so largely uncontrolled, and often even is unknown, can vastly enlarge his mastery over the internal affairs of the country by his own commitment of the Nation's armed forces to some foreign venture." *Id.* at 642.

Moreover, President Truman's action extended the President's authority into a field that the Constitution predominantly assigns to Congress. *See id.* at 588 (discussing Congress's commerce power and noting that "[t]he Constitution does not subject this lawmaking power of Congress to presidential or military supervision or control"); *see also id.* at 643 (Jackson, J., concurring) (explaining that Congress is given express authority to "'raise and *support* Armies'" and "'to *provide* and *maintain* a Navy'") (quoting U.S. Const. art. I, § 8, cls. 12, 13). Thus, *Youngstown* involved an assertion of executive power that not only stretched far beyond the

President's core Commander in Chief functions, but that did so by intruding into areas where Congress had been given an express, and apparently dominant, role by the Constitution.[16]

The present situation differs dramatically. The exercise of executive authority involved in the NSA activities is not several steps removed from the actual conduct of a military campaign. As explained above, it is an essential part of the military campaign. Unlike the activities at issue in *Youngstown*, the NSA activities are directed at the enemy, and not at domestic activity that might incidentally aid the war effort. And assertion of executive authority here does not involve extending presidential power into areas reserved for Congress. Moreover, the theme that appeared most strongly in Justice Jackson's concurrence in *Youngstown*—the fear of presidential bootstrapping—does not apply in this context. Whereas President Truman had used his inherent constitutional authority to commit U.S. troops, here Congress expressly provided the President sweeping authority to use "all necessary and appropriate force" to protect the Nation from further attack. AUMF § 2(a). There is thus no bootstrapping concern.

Finally, *Youngstown* cannot be read to suggest that the President's authority for engaging the enemy is less extensive inside the United States than abroad. To the contrary, the extent of the President's Commander in Chief authority necessarily depends on where the enemy is found and where the battle is waged. In World War II, for example, the Supreme Court recognized that the President's authority as Commander in Chief, as supplemented by Congress, included the power to capture and try agents of the enemy in the United States, even if they never had "entered the theatre or zone of active military operations." *Quirin,* 317 U.S. at 38.[17] In the present conflict, unlike in the Korean War, the battlefield was brought to the United States in the most literal way, and the United States continues to face a threat of further attacks on its soil. In short, therefore, *Youngstown* does not support the view that Congress may constitutionally prohibit the President from authorizing the NSA activities.

The second serious constitutional question is whether the particular restrictions imposed by FISA would impermissibly hamper the President's exercise of his constitutionally assigned duties as Commander in Chief. The President has determined that the speed and agility required to carry out the NSA activities successfully could not have been achieved under FISA.[18] Because the President also has determined that the NSA activities are necessary to the defense of the United States from a subsequent terrorist attack in the armed conflict with al Qaeda, FISA would impermissibly interfere with the President's most solemn constitutional obligation—to defend the United States against foreign attack.

---

[16] *Youngstown* does demonstrate that the mere fact that Executive action might be placed in Justice Jackson's category III does not obviate the need for further analysis. Justice Jackson's framework therefore recognizes that Congress might impermissibly interfere with the President's authority as Commander in Chief or to conduct the Nation's foreign affairs.

[17] It had been recognized long before *Youngstown* that, in a large-scale conflict, the area of operations could readily extend to the continental United States, even when there are no major engagements of armed forces here. Thus, in the context of the trial of a German officer for spying in World War I, it was recognized that "[w]ith the progress made in obtaining ways and means for devastation and destruction, the territory of the United States was certainly within the field of active operations" during the war, particularly in the port of New York, and that a spy in the United States might easily have aided the "hostile operation" of U-boats off the coast. *United States ex rel. Wessels v. McDonald,* 265 F. 754, 764 (E.D.N.Y. 1920).

[18] In order to avoid further compromising vital national security activities, a full explanation of the basis for the President's determination cannot be given in an unclassified document.

Indeed, if an interpretation of FISA that allows the President to conduct the NSA activities were not "fairly possible," FISA would be unconstitutional as applied in the context of this congressionally authorized armed conflict. In that event, FISA would purport to *prohibit* the President from undertaking actions necessary to fulfill his constitutional obligation to protect the Nation from foreign attack in the context of a congressionally authorized armed conflict with an enemy that has already staged the most deadly foreign attack in our Nation's history. A statute may not "*impede* the President's ability to perform his constitutional duty," *Morrison v. Olson*, 487 U.S. 654, 691 (1988) (emphasis added); *see also id.* at 696-97, particularly not the President's most solemn constitutional obligation—the defense of the Nation. *See also In re Sealed Case*, 310 F.3d at 742 (explaining that "FISA could not encroach on the President's constitutional power").

Application of the avoidance canon would be especially appropriate here for several reasons beyond the acute constitutional crises that would otherwise result. First, as noted, Congress did not intend FISA to be the final word on electronic surveillance conducted during armed conflicts. Instead, Congress expected that it would revisit the subject in subsequent legislation. Whatever intent can be gleaned from FISA's text and legislative history to set forth a comprehensive scheme for regulating electronic surveillance during peacetime, that same intent simply does not extend to armed conflicts and declared wars.[19] Second, FISA was enacted during the Cold War, not during active hostilities with an adversary whose mode of operation is to blend in with the civilian population until it is ready to strike. These changed circumstances have seriously altered the constitutional calculus, one that FISA's enactors had already recognized might suggest that the statute was unconstitutional. Third, certain technological changes have rendered FISA still more problematic. As discussed above, when FISA was enacted in 1978, Congress expressly declined to regulate through FISA certain signals intelligence activities conducted by the NSA. *See supra*, at pp. 18-19 & n.6.[20] These same factors weigh heavily in favor of concluding that FISA would be unconstitutional as applied to the current conflict if the canon of constitutional avoidance could not be used to head off a collision between the Branches.

---

[19] FISA exempts the President from its procedures for fifteen days following a congressional declaration of war. *See* 50 U.S.C. § 1811. If an adversary succeeded in a decapitation strike, preventing Congress from declaring war or passing subsequent authorizing legislation, it seems clear that FISA could not constitutionally continue to apply in such circumstances.

[20] Since FISA's enactment in 1978, the means of transmitting communications has undergone extensive transformation. In particular, many communications that would have been carried by wire are now transmitted through the air, and many communications that would have been carried by radio signals (including by satellite transmissions) are now transmitted by fiber optic cables. It is such technological advancements that have broadened FISA's reach, not any particularized congressional judgment that the NSA's traditional activities in intercepting such international communications should be subject to FISA's procedures. A full explanation of these technological changes would require a discussion of classified information.

* * *

As explained above, FISA is best interpreted to allow a statute such as the AUMF to authorize electronic surveillance outside FISA's enumerated procedures. The strongest counterarguments to this conclusion are that various provisions in FISA and title 18, including section 111 of FISA and section 2511(2)(f) of title 18, together require that subsequent legislation must reference or amend FISA in order to authorize electronic surveillance outside FISA's procedures and that interpreting the AUMF as a statute authorizing electronic surveillance outside FISA procedures amounts to a disfavored repeal by implication. At the very least, however, interpreting FISA to allow a subsequent statute such as the AUMF to authorize electronic surveillance without following FISA's express procedures is "fairly possible," and that is all that is required for purposes of invoking constitutional avoidance. In the competition of competing canons, particularly in the context of an ongoing armed conflict, the constitutional avoidance canon carries much greater interpretative force.[21]

IV. THE NSA ACTIVITIES ARE CONSISTENT WITH THE FOURTH AMENDMENT

The Fourth Amendment prohibits "unreasonable searches and seizures" and directs that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. The touchstone for review of government action under the Fourth Amendment is whether the search is "reasonable." *See, e.g., Vernonia Sch. Dist. v. Acton,* 515 U.S. 646, 653 (1995).

---

[21] If the text of FISA were clear that nothing other than an amendment to FISA could authorize additional electronic surveillance, the AUMF would impliedly repeal as much of FISA as would prevent the President from using "all necessary and appropriate force" in order to prevent al Qaeda and its allies from launching another terrorist attack against the United States. To be sure, repeals by implication are disfavored and are generally not found whenever two statutes are "capable of co-existence." *Ruckelshaus v. Monsanto Co.*, 467 U.S. 986, 1018 (1984). Under this standard, an implied repeal may be found where one statute would "unduly interfere with" the operation of another. *Radzanower v. Touche Ross & Co.*, 426 U.S. 148, 156 (1976). The President's determination that electronic surveillance of al Qaeda outside the confines of FISA was "necessary and appropriate" would create a clear conflict between the AUMF and FISA. FISA's restrictions on the use of electronic surveillance would preclude the President from doing what the AUMF specifically authorized him to do: use all "necessary and appropriate force" to prevent al Qaeda from carrying out future attacks against the United States. The ordinary restrictions in FISA cannot continue to apply if the AUMF is to have its full effect; those constraints would "unduly interfere" with the operation of the AUMF.

Contrary to the recent suggestion made by several law professors and former government officials, the ordinary presumption against implied repeals is overcome here. *Cf.* Letter to the Hon. Bill Frist, Majority Leader, U.S. Senate, from Professor Curtis A. Bradley et al. at 4 (Jan. 9, 2006). First, like other canons of statutory construction, the canon against implied repeals is simply a presumption that may be rebutted by other factors, including conflicting canons. *Connecticut National Bank v. Germain*, 503 U.S. 249, 253 (1992); *see also Chickasaw Nation v. United States*, 534 U.S. 84, 94 (2001); *Circuit City Stores, Inc. v. Adams*, 532 U.S. 105, 115 (2001). Indeed, the Supreme Court has declined to apply the ordinary presumption against implied repeals where other canons apply and suggest the opposite result. *See Montana v. Blackfeet Tribe of Indians*, 471 U.S. 759, 765-66 (1985). Moreover, *Blackfeet* suggests that where the presumption against implied repeals would conflict with other, more compelling interpretive imperatives, it simply does not apply at all. *See* 471 U.S. at 766. Here, in light of the constitutional avoidance canon, which imposes the overriding imperative to use the tools of statutory interpretation to avoid constitutional conflicts, the implied repeal canon either would not apply at all or would apply with significantly reduced force. Second, the AUMF was enacted during an acute national emergency, where the type of deliberation and detail normally required for application of the canon against implied repeals was neither practical nor warranted. As discussed above, in these circumstances, Congress cannot be expected to work through every potential implication of the U.S. Code and to define with particularity each of the traditional incidents of the use of force available to the President.

As noted above, *see* Part I, all of the federal courts of appeals to have addressed the issue have affirmed the President's inherent constitutional authority to collect foreign intelligence without a warrant. *See In re Sealed Case,* 310 F.3d at 742. Properly understood, foreign intelligence collection in general, and the NSA activities in particular, fit within the "special needs" exception to the warrant requirement of the Fourth Amendment. Accordingly, the mere fact that no warrant is secured prior to the surveillance at issue in the NSA activities does not suffice to render the activities unreasonable. Instead, reasonableness in this context must be assessed under a general balancing approach, "'by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.'" *United States v. Knights*, 534 U.S. 112, 118-19 (2001) (quoting *Wyoming v. Houghton*, 526 U.S. 295, 300 (1999)). The NSA activities are reasonable because the Government's interest, defending the Nation from another foreign attack in time of armed conflict, outweighs the individual privacy interests at stake, and because they seek to intercept only international communications where one party is linked to al Qaeda or an affiliated terrorist organization.

A. THE WARRANT REQUIREMENT OF THE FOURTH AMENDMENT DOES NOT APPLY TO THE NSA ACTIVITIES

In "the criminal context," the Fourth Amendment reasonableness requirement "usually requires a showing of probable cause" and a warrant. *Board of Educ. v. Earls,* 536 U.S. 822, 828 (2002). The requirement of a warrant supported by probable cause, however, is not universal. Rather, the Fourth Amendment's "central requirement is one of reasonableness," and the rules the Court has developed to implement that requirement "[s]ometimes . . . require warrants." *Illinois v. McArthur*, 531 U.S. 326, 330 (2001); *see also, e.g., Earls*, 536 U.S. at 828 (noting that the probable cause standard "is peculiarly related to criminal investigations and may be unsuited to determining the reasonableness of administrative searches where the Government seeks to prevent the development of hazardous conditions") (internal quotation marks omitted).

In particular, the Supreme Court repeatedly has made clear that in situations involving "special needs" that go beyond a routine interest in law enforcement, the warrant requirement is inapplicable. *See Vernonia,* 515 U.S. at 653 (there are circumstances "'when special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable'") (quoting *Griffin* v. *Wisconsin,* 483 U.S. 868, 873 (1987)); *see also McArthur,* 531 U.S. at 330 ("When faced with special law enforcement needs, diminished expectations of privacy, minimal intrusions, or the like, the Court has found that certain general, or individual, circumstances may render a warrantless search or seizure reasonable."). It is difficult to encapsulate in a nutshell all of the different circumstances the Court has found to qualify as "special needs" justifying warrantless searches. But one application in which the Court has found the warrant requirement inapplicable is in circumstances in which the Government faces an increased need to be able to react swiftly and flexibly, or when there are at stake interests in public safety beyond the interests in ordinary law enforcement. One important factor in establishing "special needs" is whether the Government is responding to an emergency that goes beyond the need for general crime control. *See In re Sealed Case*, 310 F.3d at 745-46.

Thus, the Court has permitted warrantless searches of property of students in public schools, *see New Jersey v. T.L.O.*, 469 U.S. 325, 340 (1985) (noting that warrant requirement would "unduly interfere with the maintenance of the swift and informal disciplinary procedures needed in the schools"), to screen athletes and students involved in extracurricular activities at public schools for drug use, *see Vernonia*, 515 U.S. at 654-55; *Earls*, 536 U.S. at 829-38, to conduct drug testing of railroad personnel involved in train accidents, *see Skinner v. Railway Labor Executives' Ass'n,* 489 U.S. 602, 634 (1989), and to search probationers' homes, *see Griffin*, 483 U.S. 868. Many special needs doctrine and related cases have upheld *suspicionless* searches or seizures. *See, e.g., Illinois v. Lidster*, 540 U.S. 419, 427 (2004) (implicitly relying on special needs doctrine to uphold use of automobile checkpoint to obtain information about recent hit-and-run accident); *Earls*, 536 U.S. at 829-38 (suspicionless drug testing of public school students involved in extracurricular activities); *Michigan Dep't of State Police v. Sitz*, 496 U.S. 444, 449-55 (1990) (road block to check all motorists for signs of drunken driving); *United States* v. *Martinez-Fuerte*, 428 U.S. 543 (1976) (road block near the border to check vehicles for illegal immigrants); *cf. In re Sealed Case*, 310 F.3d at 745-46 (noting that suspicionless searches and seizures in one sense are a greater encroachment on privacy than electronic surveillance under FISA because they are not based on any particular suspicion, but "[o]n the other hand, wiretapping is a good deal more intrusive than an automobile stop accompanied by questioning"). To fall within the "special needs" exception to the warrant requirement, the purpose of the search must be distinguishable from ordinary general crime control. *See, e.g., Ferguson v. Charleston*, 532 U.S. 67 (2001); *City of Indianapolis v. Edmond*, 531 U.S. 32, 41 (2000).

Foreign intelligence collection, especially in the midst of an armed conflict in which the adversary has already launched catastrophic attacks within the United States, fits squarely within the area of "special needs, beyond the normal need for law enforcement" where the Fourth Amendment's touchstone of reasonableness can be satisfied without resort to a warrant. *Vernonia*, 515 U.S. at 653. The Executive Branch has long maintained that collecting foreign intelligence is far removed from the ordinary criminal law enforcement action to which the warrant requirement is particularly suited. *See, e.g.*, Amending the Foreign Intelligence Surveillance Act: Hearings Before the House Permanent Select Comm. on Intelligence,103d Cong. 2d Sess. 62, 63 (1994) (statement of Deputy Attorney General Jamie S. Gorelick) ("[I]t is important to understand that the rules and methodology for criminal searches are inconsistent with the collection of foreign intelligence and would unduly frustrate the President in carrying out his foreign intelligence responsibilities. . . . [W]e believe that the warrant clause of the Fourth Amendment is inapplicable to such [foreign intelligence] searches."); *see also In re Sealed Case*, 310 F.3d 745. The object of foreign intelligence collection is securing information necessary to protect the national security from the hostile designs of foreign powers like al Qaeda and affiliated terrorist organizations, including the possibility of another foreign attack on the United States. In foreign intelligence investigations, moreover, the targets of surveillance often are agents of foreign powers, including international terrorist groups, who may be specially trained in concealing their activities and whose activities may be particularly difficult to detect. The Executive requires a greater degree of flexibility in this field to respond with speed and absolute secrecy to the ever-changing array of foreign threats faced by the Nation.[22]

In particular, the NSA activities are undertaken to prevent further devastating attacks on our Nation, and they serve the highest government purpose through means other than traditional law enforcement.[23] The NSA activities are designed to enable the Government to act quickly and flexibly (and with secrecy) to find agents of al Qaeda and its affiliates—an international terrorist group which has already demonstrated a capability to infiltrate American communities without being detected—in time to disrupt future terrorist attacks against the United States. As explained by the Foreign Intelligence Surveillance Court of Review, the nature of the "emergency" posed by al Qaeda "takes the matter out of the realm of ordinary crime control." *In re Sealed Case*, 310 F.3d at 746. Thus, under the "special needs" doctrine, no warrant is required by the Fourth Amendment for the NSA activities.

B. THE NSA ACTIVITIES ARE REASONABLE

As the Supreme Court has emphasized repeatedly, "[t]he touchstone of the Fourth Amendment is reasonableness, and the reasonableness of a search is determined by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests." *Knights*, 534 U.S. at 118-19 (quotation marks omitted); *see also Earls,* 536 U.S. at 829. The Supreme Court has found a search reasonable when, under the totality of the circumstances, the importance of the governmental interests outweighs the nature and quality of the intrusion on the individual's Fourth Amendment interests. *See Knights*, 534 U.S. at 118-22. Under the standard

[22] Even in the domestic context, the Supreme Court has recognized that there may be significant distinctions between wiretapping for ordinary law enforcement purposes and domestic national security surveillance. *See United States v. United States District Court,* 407 U.S. 297, 322 (1972) ("*Keith*") (explaining that "the focus of domestic [security] surveillance may be less precise than that directed against more conventional types of crime" because often "the emphasis of domestic intelligence gathering is on the prevention of unlawful activity or the enhancement of the Government's preparedness for some possible future crisis or emergency"); *see also United States v. Duggan*, 743 F.2d 59, 72 (2d Cir. 1984) (reading *Keith* to recognize that "the governmental interests presented in national security investigations differ substantially from those presented in traditional criminal investigations"). Although the Court in *Keith* held that the Fourth Amendment's warrant requirement does apply to investigations of purely *domestic* threats to national security—such as domestic terrorism, it suggested that Congress consider establishing a lower standard for such warrants than that set forth in Title III. *See id.* at 322-23 (advising that "different standards" from those applied to traditional law enforcement "may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of the Government for intelligence information and the protected rights of our citizens"). *Keith*'s emphasis on the need for flexibility applies with even greater force to surveillance directed at *foreign* threats to national security. *See* S. Rep. No. 95-701, at 16 ("Far more than in domestic security matters, foreign counterintelligence investigations are 'long range' and involve 'the interrelation of various sources and types of information.'") (quoting *Keith*, 407 U.S. at 322). And flexibility is particularly essential here, where the purpose of the NSA activities is to prevent another armed attack against the United States.

[23] This is not to say that traditional law enforcement has no role in protecting the Nation from attack. The NSA activities, however, are not directed at bringing criminals to justice but at detecting and preventing plots by a declared enemy of the United States to attack it again.

balancing of interests analysis used for gauging reasonableness, the NSA activities are consistent with the Fourth Amendment.

With respect to the individual privacy interests at stake, there can be no doubt that, as a general matter, interception of telephone communications implicates a significant privacy interest of the individual whose conversation is intercepted. The Supreme Court has made clear at least since *Katz v. United States,* 389 U.S. 347 (1967), that individuals have a substantial and constitutionally protected reasonable expectation of privacy that their telephone conversations will not be subject to governmental eavesdropping. Although the individual privacy interests at stake may be substantial, it is well recognized that a variety of governmental interests—including routine law enforcement and foreign-intelligence gathering—can overcome those interests.

On the other side of the scale here, the Government's interest in engaging in the NSA activities is the most compelling interest possible—securing the Nation from foreign attack in the midst of an armed conflict. One attack already has taken thousands of lives and placed the Nation in state of armed conflict. Defending the Nation from attack is perhaps the most important function of the federal Government—and one of the few express obligations of the federal Government enshrined in the Constitution. *See* U.S. Const. art. IV, § 4 ("The United States shall guarantee to every State in this Union a Republican Form of Government, *and shall protect each of them against Invasion* . . . .") (emphasis added); *The Prize Cases*, 67 U.S. (2 Black) 635, 668 (1863) ("If war be made by invasion of a foreign nation, the President is not only authorized but bound to resist force by force."). As the Supreme Court has declared, "[i]t is 'obvious and unarguable' that no governmental interest is more compelling than the security of the Nation." *Haig v. Agee,* 453 U.S. 280, 307 (1981).

The Government's overwhelming interest in detecting and thwarting further al Qaeda attacks is easily sufficient to make reasonable the intrusion into privacy involved in intercepting one-end foreign communications where there is "a reasonable basis to conclude that one party to the communication is a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda." Press Briefing by Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence, *available at* http://www.whitehouse.gov/news/releases/2005/12/20051219-1.html (Dec. 19, 2005) (statement of Attorney General Gonzales); *cf. Edmond*, 531 U.S. at 44 (noting that "the Fourth Amendment would almost certainly permit an appropriately tailored roadblock set up to thwart an imminent terrorist attack" because "[t]he exigencies created by th[at] scenario[] are far removed" from ordinary law enforcement). The United States has already suffered one attack that killed thousands, disrupted the Nation's financial center for days, and successfully struck at the command and control center for the Nation's military. And the President has stated that the NSA activities are "critical" to our national security. Press Conference of President Bush (Dec. 19, 2005). To this day, finding al Qaeda sleeper agents in the United States remains one of the preeminent concerns of the war on terrorism. As the President has explained, "[t]he terrorists want to strike America again, and they hope to inflict even more damage than they did on September 11th." *Id.*

Of course, because the magnitude of the Government's interest here depends in part upon the threat posed by al Qaeda, it might be possible for the weight that interest carries in the balance to change over time. It is thus significant for the reasonableness of the NSA activities that the President has established a system under which he authorizes the surveillance only for a limited period, typically for 45 days. This process of reauthorization ensures a periodic review to evaluate whether the threat from al Qaeda remains sufficiently strong that the Government's interest in protecting the Nation and its citizens from foreign attack continues to outweigh the individual privacy interests at stake.

Finally, as part of the balancing of interests to evaluate Fourth Amendment reasonableness, it is significant that the NSA activities are limited to intercepting international communications where there is a reasonable basis to conclude that one party to the communication is a member or agent of al Qaeda or an affiliated terrorist organization. This factor is relevant because the Supreme Court has indicated that in evaluating reasonableness, one should consider the "efficacy of [the] means for addressing the problem." *Vernonia*, 515 U.S. at 663; *see also Earls,* 536 U.S. at 834 ("Finally, this Court must consider the nature and immediacy of the government's concerns and the efficacy of the Policy in meeting them."). That consideration does not mean that reasonableness requires the "least intrusive" or most "narrowly tailored" means for obtaining information. To the contrary, the Supreme Court has repeatedly rejected such suggestions. *See, e.g., Earls,* 536 U.S. at 837 ("[T]his Court has repeatedly stated that reasonableness under the Fourth Amendment does not require employing the least intrusive means, because the logic of such elaborate less-restrictive-alternative arguments could raise insuperable barriers to the exercise of virtually all search-and-seizure powers.") (internal quotation marks omitted); *Vernonia,* 515 U.S. at 663 ("We have repeatedly refused to declare that only the 'least intrusive' search practicable can be reasonable under the Fourth Amendment."). Nevertheless, the Court has indicated that some consideration of the efficacy of the search being implemented—that is, some measure of fit between the search and the desired objective—is relevant to the reasonableness analysis. The NSA activities are targeted to intercept international communications of persons reasonably believed to be members or agents of al Qaeda or an affiliated terrorist organization, a limitation which further strongly supports the reasonableness of the searches.

In sum, the NSA activities are consistent with the Fourth Amendment because the warrant requirement does not apply in these circumstances, which involve both "special needs" beyond the need for ordinary law enforcement and the inherent authority of the President to conduct warrantless electronic surveillance to obtain foreign intelligence to protect our Nation from foreign armed attack. The touchstone of the Fourth Amendment is reasonableness, and the NSA activities are certainly reasonable, particularly taking into account the nature of the threat the Nation faces.

CONCLUSION

For the foregoing reasons, the President—in light of the broad authority to use military force in response to the attacks of September 11th and to prevent further catastrophic attack expressly conferred on the President by the Constitution and confirmed and supplemented by

Congress in the AUMF—has legal authority to authorize the NSA to conduct the signals intelligence activities he has described. Those activities are authorized by the Constitution and by statute, and they violate neither FISA nor the Fourth Amendment.

EXHIBIT J

THE WHITE HOUSE
PRESIDENT GEORGE W. BUSH

For Immediate Release
Office of the Press Secretary
December 19, 2005

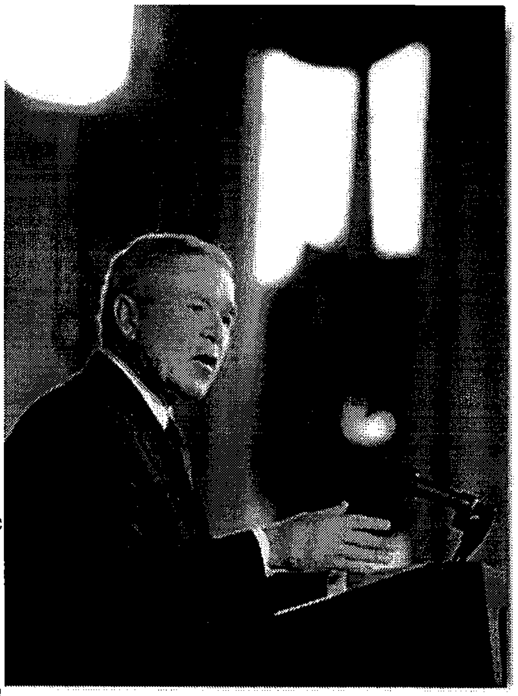
Press Conference of the President

The East Room

10:32 A.M. EST

THE PRESIDENT: Welcome. Please be seated. Thanks.

Last night I addressed the nation about our strategy for victory in Iraq, and the historic elections that took place in the country last week. In a nation that once lived by the whims of a brutal dictator, the Iraqi people now enjoy constitutionally protected freedoms, and their leaders now derive their powers from the consent of the government. Millions of Iraqis are looking forward to a future with hope and optimism.



The Iraqi people still face many challenges. This is the first time the Iraqis are forming a government under their new constitution. The Iraqi constitution requires a two-thirds vote of the parliament for certain top officials. So the formation of the new government will take time as Iraqis work to build consensus. And once the new Iraqi government assumes office, Iraq's new leaders will face many important decisions on issues such as security and reconstruction, economic reform and national unity. The work ahead will require the patience of the Iraqi people and the patience and support of America and our coalition partners.

As I said last night, this election does not mean the end of violence, but it is the beginning of something new: a constitutional democracy at the heart of the Middle East. And we will keep working toward our goal of a democratic Iraq that can govern and self-sustain itself and defend itself.

Our mission in Iraq is critical in the victory in the global war on terror. After our country was attacked on September the 11th and nearly 3,000 lives were lost, I vowed to do everything within my power to bring justice to those who were responsible. I also pledged to the American people to do everything within my power to prevent this from happening again. What we quickly learned was that al Qaeda was not a conventional enemy. Some lived in our cities and communities, and communicated from here in America to plot and plan with bin Laden's lieutenants in Afghanistan, Pakistan and elsewhere. Then they boarded our airplanes and launched the worst attack on our country in our nation's history.

question that you didn't seem to have an answer for the last time you were asked, and that is, what would you say is the biggest mistake you've made during your presidency, and what have you learned from it?

THE PRESIDENT: Answering Dickerson's question. No, I -- the last time those questions were asked, I really felt like it was an attempt for me to say it was a mistake to go into Iraq. And it wasn't a mistake to go into Iraq. It was the right decision to make.

I think that, John, there's going to be a lot of analysis done on the decisions on the ground in Iraq. For example, I'm fully aware that some have said it was a mistake not to put enough troops there immediately -- or more troops. I made my decision based upon the recommendations of Tommy Franks, and I still think it was the right decision to make. But history will judge.

I said the other day that a mistake was trying to train a civilian defense force and an Iraqi army at the same time, but not giving the civilian defense force enough training and tools necessary to be able to battle a group of thugs and killers. And so we adjusted.

And the point I'm trying to make to the American people in this, as you said, candid dialogue -- I hope I've been candid all along; but in the candid dialogue -- is to say, we're constantly changing our tactics to meet the changing tactics of an enemy. And that's important for our citizens to understand.

Thank you. Kelly.

Q Thank you, Mr. President. If you believe that present law needs to be faster, more agile concerning the surveillance of conversations from someone in the United States to someone outside the country --

THE PRESIDENT: Right.

Q -- why, in the four years since 9/11, has your administration not sought to get changes in the law instead of bypassing it, as some of your critics have said?

THE PRESIDENT: I appreciate that. First, I want to make clear to the people listening that this program is limited in nature to those that are known al Qaeda ties and/or affiliates. That's important. So it's a program that's limited, and you brought up something that I want to stress, and that is, is that these calls are not intercepted within the country. They are from outside the country to in the country, or vice versa. So in other words, this is not a -- if you're calling from Houston to L.A., that call is not monitored. And if there was ever any need to monitor, there would be a process to do that.

I think I've got the authority to move forward, Kelly. I mean, this is what -- and the Attorney General was out briefing this morning about why it's legal to make the decisions I'm making. I can fully understand why members of Congress are expressing concerns about civil liberties. I know that. And it's -- I share the same concerns. I want to make sure the American people understand, however, that we have an obligation to protect you, and we're doing that and, at the same time, protecting your civil liberties.

Secondly, an open debate about law would say to the enemy, here is what we're going to do. And this is an enemy which adjusts. We monitor this program carefully. We have consulted with members of the Congress over a dozen times. We are constantly reviewing the program. Those of us who review the program have a duty to uphold the laws of the United States, and we take that duty very seriously.

Let's see here -- Martha. Working my way around the electronic media, here.